

# EMC® NetWorker®

Version 8.2

## Administration Guide

302-000-688

REV 05



**EMC<sup>2</sup>**

Copyright © 1990-2014 EMC Corporation. All rights reserved. Published in USA.

Published November, 2014

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.

EMC<sup>2</sup>, 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](http://www.EMC.com)

# CONTENTS

<b>Figures</b>	<b>23</b>	
<b>Tables</b>	<b>25</b>	
<b>Preface</b>	<b>29</b>	
<b>Chapter 1</b>	<b>Overview</b>	<b>33</b>
	The NetWorker environment.....	34
	NetWorker components.....	34
	NetWorker features.....	35
	Performance features.....	35
	Ease of use.....	36
	Scalability.....	37
	Optional software additions.....	37
	NetWorker user interfaces.....	37
	NetWorker Management Console interface.....	37
	NetWorker client interface.....	45
	NetWorker character-based interface.....	48
	NetWorker command-line interface.....	48
	Common NetWorker tasks.....	48
	Adding a new host.....	48
	Device configuration.....	48
	Labelling media.....	50
	Scheduling a backup.....	50
	Viewing failed backups.....	50
	Performing a manual backup.....	51
	NetWorker services.....	52
	Services and programs on the NetWorker server.....	52
	Services and programs on the NetWorker client.....	53
	Services and programs on the NetWorker storage node .....	53
	Services and programs on the NetWorker Management Console server .....	54
	Stop and start the NMC server.....	54
	Stop and start a NetWorker server, client, or storage node.....	55
<b>Chapter 2</b>	<b>Backing Up Data</b>	<b>59</b>
	Scheduled backups.....	60
	Scheduled backup planning.....	60
	Scheduled backup creation.....	61
	Manual scheduled backup creation in the Console.....	62
	Setting up policies for quick access and long term storage.....	64
	Setting up a label template to identify volumes.....	64
	Setting up directives for special processing.....	65
	Creating a backup Client resource.....	65
	Setting up a pool to sort backup data.....	67
	Creating Schedules.....	68
	Save sets.....	68

Predefined save sets for scheduled backups.....	69
The ALL save set.....	69
Manual backups.....	71
Performing a manual backup on Windows.....	71
Performing a manual backup from the command prompt.....	72
Verifying backup data.....	73
Synthetic full backups.....	73
Differences between a synthetic full backup and a traditional backup .....	74
When to use synthetic full backups.....	74
How a synthetic full backup is created.....	75
Synthetic full requirements.....	76
Limitations of synthetic full backups.....	77
Recommended devices for synthetic full backups.....	78
Synthetic full scheduling considerations.....	78
Synthetic full and backup levels.....	79
Synthetic full backups.....	79
Checking the integrity of a synthetic full backup .....	82
Checkpoint restart considerations with synthetic full backups.....	83
Synthetic full backup reporting.....	83
Running queries on synthetic full backups.....	83
Monitoring.....	83
Directives.....	84
Directing data from a synthetic full backup to a dedicated pool.....	84
Virtual synthetic full backups (for Data Domain systems).....	84
Virtual synthetic full requirements.....	85
Enable/disable VSF in NMC.....	86
Performing VSF.....	86
Directives.....	86
Multiple storage node distribution.....	86
Concurrent operations.....	87
VSF validation .....	87
VSF limitations .....	88
Enabling parallel save streams.....	89
Troubleshooting PSS.....	89
Probe-based backups.....	90
Configuring a probe-based backup group.....	90
Creating a client probe .....	91
Associating a probe with a Client resource.....	91
Client Direct backups.....	92
Checkpoint restart backups.....	92
Checkpoint restart usage.....	92
About partial non-NDMP save sets.....	93
About partial NDMP save sets.....	94
Configuring checkpoint enabled clients.....	94
Restart checkpoint-enabled backups.....	95
Monitoring checkpoint-enabled backups.....	97
Checkpoint-enabled backup reporting.....	97
Query the media database for partial save sets.....	99
Checkpoint restart data recovery.....	101
Partial saveset cloning and scanning.....	102
Cloud backup devices and partial savesets.....	102
Deduplication backups.....	102
Backup data encryption.....	102
Microsoft Encrypting File System (EFS) and NetWorker AES encryption .....	102

Setting the Datazone pass phrase for a NetWorker server.....	103
Apply AES data encryption to clients in the datazone.....	103
Backup data compression.....	103
Applying compression to a scheduled backup.....	103
Applying compression to a manual backup.....	103
Handling data for NetWorker clients on Windows.....	104
Console server management data backups.....	104
Scheduling backups for the Console server database.....	104
Performing a manual backup of the Console database.....	105
Managing the size of the Console database log file.....	106
Windows mount point back ups.....	106
Including mount points in scheduled backups.....	106
Performing a manual backup of a mount point and its data.....	107
Performing a manual backup of nested mount points and their data.....	107
Windows Content Index Server or Windows Search Index backups.....	108
Back up CIS or Windows Search on Windows.....	108
Directing NetWorker software to skip CIS or Windows Search catalog backups.....	109
Backing up Windows DHCP and WINS databases.....	109
Windows backup and recovery notes.....	109
Enabling short filename support.....	109
Enabling hard link support on a NetWorker client.....	110
Failed backup and recovery attempts.....	110
Granting full permissions for backup of Disk Quota database.....	110
Native VHD volume support.....	111
Avoiding recovery problems with case-sensitivity.....	111
Enabling NetWorker logging operations performed by backup operator.....	111
Customizing the backup command.....	112
Creating a custom backup script.....	113
Example 1: The save backup command on Windows.....	113
Example 2: The save backup command on UNIX.....	115
Controlling the custom backup script exit status reporting.....	116
Using the savepnpc command with a customized backup program.....	117
Considerations for backing up raw partitions.....	120
Backing up raw partitions on UNIX.....	120
Backing up raw partitions on Windows.....	120
Backing up access control lists.....	121
BOOT/BCD Data on Windows backups.....	121
Support for backing up renamed directories.....	121
Backing up only client file indexes and the bootstrap.....	122
<b>Chapter 3</b>	
<b>Storage Nodes and Libraries</b>	<b>123</b>
Storage nodes.....	124
Requirements.....	124
Licensing.....	124
Storage node configuration.....	124
Configuring a storage node.....	124
Modifying the timeout attribute for storage node operations.....	126
Configuring timeouts for storage node remote devices.....	127
Configuring the client's storage node affinity list.....	127
Balancing the load on the storage node.....	128
Bootstrap backup on a storage node.....	130

Dedicated storage nodes.....	130
Troubleshooting storage nodes.....	131
Avamar deduplication nodes and replication nodes.....	131
Devices and libraries.....	131
SCSI libraries.....	131
NDMP libraries.....	132
Silo libraries.....	132
Autodetection of libraries and tape devices.....	132
Scanning for libraries and devices.....	132
Refreshing enterprise library views on request.....	134
Changing the polling interval for enterprise library views.....	134
Configure libraries.....	134
Adding a library resource.....	135
Virtual tape library (VTL) configuration.....	135
Queuing device resources for AlphaStor.....	136
Reconfigure libraries.....	136
Reconfiguring a library.....	136
Library configuration using the jedit command.....	137
Specify available library slots.....	137
Specifying library slots.....	137
Miscellaneous library operations.....	138
NetWorker hosts with shared libraries.....	138
Library task inactivity periods.....	139
Server Network Interface attribute.....	140
Tips for using libraries.....	140
Library notifications.....	140
Reset a library.....	141
Pools with libraries.....	141
Adding and removing media by using the library front panel.....	142
Library maintenance.....	142
Automatic tape device cleaning.....	142
Selecting a tape device manually for cleaning.....	143
Delaying tape device cleaning.....	143
Tape alert.....	143
Deleting libraries.....	145
Troubleshooting autoconfiguration failure.....	145
Silo libraries.....	146
NetWorker software interactions with a silo.....	146
Installing a silo.....	146
Naming conventions for silo devices.....	146
Configuring silo libraries.....	147
NetWorker software with ACSLS silos.....	148
Releasing a silo device.....	149
Silo device cleaning.....	149
Environment variables for StorageTek silos.....	149
<b>Chapter 4</b>	
<b>Backup to Disk and Cloud</b>	<b>151</b>
Types of disk storage devices.....	152
FTD.....	152
AFTD.....	152
DD Boost devices.....	152
Cloud.....	153
Example environment.....	153
Differences between FTDs, AFTDs, and DD Boost devices.....	153
File type devices.....	156



	Support for LTO-4 hardware-based encryption.....	200
	Whether to add or recycle volumes.....	200
	Displaying device operations messages.....	201
	Device Service mode.....	201
	Setting the Service mode for a device.....	201
<b>Chapter 6</b>	<b>Media Management</b>	<b>203</b>
	Storage management operations.....	204
	How the NetWorker server uses volume labels.....	204
	Selecting a volume for the NetWorker server.....	204
	Auto Media Management.....	206
	Existing tapes with NetWorker labels.....	206
	Auto Media Management for stand-alone devices.....	206
	Volume operations.....	207
	Viewing volume status information.....	208
	Read-only mode.....	209
	Recycle volumes.....	210
	Volume labels.....	210
	Empty slots in label operations.....	212
	Volume mounting and unmounting.....	214
	Libraries with volume import and export capability.....	218
	Inventorying library volumes.....	219
	Remove volumes from the media database and online indexes.....	220
	Media handling errors.....	222
	Re-enabling a device.....	222
	Media management in a silo.....	223
	Silo slot numbering.....	223
	Silo volume mounting and unmounting.....	223
	Silo volume labeling.....	223
	Using silos with volume import and export capability.....	224
	Barcode IDs.....	224
	Inventory silos.....	227
	Volume save sets.....	227
	Viewing save set details in the Volume Save Sets window.....	227
	Viewing save set details from the save set detail table.....	229
<b>Chapter 7</b>	<b>Browse and Retention Policies</b>	<b>231</b>
	About browse and retention policies.....	232
	Browse policies.....	232
	Retention policies.....	234
	Managing the data lifecycle.....	236
	Assigning multiple policies to a single client.....	237
	Preconfigured time policies.....	238
	Editing a time policy.....	238
	Deleting a time policy.....	238
	Snapshot policies.....	238
	Working with snapshot policies.....	239
	Browse and retention policies for manual backups.....	240
	Modifying the browse and retention policy on a save set.....	241
	Changing browse and retention policies with nsrmm examples.....	241
	Reports on browse and retention policies for save sets.....	241
<b>Chapter 8</b>	<b>Backup Groups and Schedules</b>	<b>243</b>

Overview of NetWorker scheduling.....	244
Backup groups.....	244
The NetWorker server and time-based backup groups.....	244
Preconfigured groups.....	246
Key Group attributes.....	246
Probe Group.....	247
Aborted backup groups.....	248
Creating a group for backup clients.....	249
Editing a group.....	249
Deleting a group.....	250
Copying a group.....	250
Copy a group with clients.....	250
Setting the backup group time interval.....	251
Limiting full backups when the time interval is less than 24 hours.	251
Considerations for running a backup group from the command line or a script.....	252
How to manage backup groups.....	253
Previewing a backup group.....	253
Moving clients between groups.....	254
Estimating save set sizes of a backup group.....	254
Backup status reports.....	254
Bootstrap report generation.....	254
Open file backups.....	255
Opening files owned by the operating system.....	255
Opening files owned by a specific application.....	256
Backing up files that change during backup.....	256
Open file backup with VSS.....	256
Schedules.....	256
Schedules for Avamar deduplication clients.....	257
Preconfigured NetWorker schedules.....	257
Backup cycles.....	258
Considerations for scheduling and planning.....	260
Scheduling large client file systems.....	260
Key components of a schedule.....	261
Working with schedules.....	262
Overriding a client's regular backup schedule.....	263
Backup levels.....	263
How NetWorker backup levels work.....	264
The NetWorker server and backup levels.....	266
<b>Chapter 9</b>	
<b>Directives</b>	<b>269</b>
Directives overview.....	270
Types of local and global directives.....	270
Global directives.....	270
NetWorker User local directives (Windows only).....	270
Local directive files.....	270
Creating a global directive resource.....	270
Editing a global directive resource.....	271
Deleting a global directive resource.....	271
Copying a global directive resource.....	271
Example directives.....	272
Applying a global directive example.....	272
Applying a NetWorker User program local directive example (Windows only).....	272
Applying a local file directive example.....	272

	Order of precedence of global and local directives.....	273
	Local directives within the NetWorker User program.....	273
	Setting up a NetWorker User program local directive.....	273
	Preconfigured global directive resources.....	274
	Format of directive statements.....	276
	Directory specifications.....	276
	ASM specifications.....	277
	Save environment keywords.....	277
	Application Specific Modules (ASMs).....	278
	Precautions when using rawasm to back up UNIX raw partitions.....	281
	File matching with multiple ASMs in a directive.....	281
<b>Chapter 10</b>	<b>Sorting Backup Data</b>	<b>283</b>
	Media pools.....	284
	Using media pools.....	284
	NetWorker media pool types.....	284
	Sorting data with media pools.....	285
	Directing client file indexes and bootstrap to a separate media pool.....	286
	Directing consolidated backup data to a specific media pool.....	286
	Meeting the criteria for more than one media pool configuration....	287
	When no customized media pool criteria is met.....	288
	Media pool configurations.....	288
	Using storage devices and media pool configuration to sort data... <td>289</td>	289
	Creating a media pool.....	290
	Managing volumes in a media pool.....	292
	Supported WORM and DLTWORM tape drives.....	292
	Working with media pools.....	297
	Label templates.....	298
	Using label templates.....	298
	Preconfigured label templates.....	299
	Guidelines for completing Label Template attributes.....	299
	Naming label templates.....	301
	Working with label templates.....	302
<b>Chapter 11</b>	<b>Archiving</b>	<b>305</b>
	Overview of archiving.....	306
	Archive requirements.....	306
	How the NetWorker server archives data.....	306
	Indexed and nonindexed archiving.....	307
	Permissions for archiving.....	308
	Enabling archive services for the client.....	308
	Enabling or restricting archive access.....	308
	Enabling public archive access.....	308
	About archive pools.....	309
	Preconfigured Indexed Archive pool and PC Archive pool.....	309
	Preconfigured archive pool.....	309
	Attributes of Archive pools.....	309
	Archiving data procedures.....	309
	Enabling archive services for a NetWorker client.....	310
	Manually archiving data.....	310
	Scheduling data archives.....	311
	Retrieving archived data.....	313
	Retrieval permissions .....	314

	Retrieving archives from a client on UNIX.....	314
	Retrieving non-indexed archives from a client on Windows.....	315
	Recovering indexed archive data from a client on Windows.....	315
	Archive request management.....	316
	Starting a scheduled archive at any time.....	316
	Stopping a scheduled archive while in progress.....	316
	Disabling a scheduled archive.....	316
	Viewing details of a scheduled archive.....	316
<b>Chapter 12</b>	<b>Cloning</b>	<b>319</b>
	Overview of cloning.....	320
	Cloning requirements .....	320
	Save set cloning.....	320
	Considerations for scheduled clone jobs.....	320
	Setting up a scheduled clone job .....	322
	Starting a scheduled clone job manually.....	324
	Monitoring scheduled clone jobs.....	324
	Setting up automatic cloning from a backup group.....	324
	Viewing the clone status of a save set.....	325
	Cloning a save set manually.....	325
	Additional manual clone operations.....	327
	Specifying browse and retention policies for clone data.....	328
	Specifying a browse and retention policy in a scheduled clone job..	328
	Specify a browse and retention policy from the command prompt..	328
	Specifying a retention policy for a Clone pool.....	329
	Volume cloning.....	329
	Creating a clone volume.....	329
	Viewing clone volume details.....	329
	Recovering cloned data.....	329
	Recovering a clone save set from the command prompt.....	330
	Recovering a save set when all cloned instances have expired.....	331
	Cloning archived data.....	332
	Setting up a scheduled clone job .....	332
	Cloning archive volumes on-demand.....	334
	Directing clones to a special storage node.....	334
	Storage node selection criteria for reading the clone data.....	334
	Storage node selection criteria and settings for writing a clone.....	335
	Storage node selection criteria for recovering cloned data.....	336
	Using file type devices for clone operations.....	337
	Differences in the cloning process.....	337
	Manual cloning with advanced file type device .....	337
	Backup-to-tape for Avamar deduplication clients.....	338
	Cloning with Data Domain devices.....	338
	Using the nsrclone command.....	338
	nsrclone option examples.....	339
<b>Chapter 13</b>	<b>Staging Backups</b>	<b>341</b>
	Save set staging.....	342
	Working with staging policies.....	342
	Creating a staging policy.....	342
	Editing a staging policy.....	344
	Copying a staging resource.....	344
	Deleting a staging policy.....	344
	Consideration for staging a bootstrap backup.....	345

	Staging and cloning from the command prompt.....	345
<b>Chapter 14</b>	<b>Recovering Filesystem Data</b>	<b>347</b>
	NetWorker recovery overview.....	348
	Local recoveries.....	348
	Directed recoveries.....	348
	Overview of NetWorker recovery methods.....	351
	Browsable recovery.....	351
	Save set recovery.....	352
	Scanner recovery.....	352
	VSS File Level Recovery.....	352
	Recovering the data.....	352
	Using the Recovery Wizard.....	353
	Using the recover command.....	358
	Using the NetWorker User program.....	361
	Using the scanner program to recover data.....	365
	Using VSS file level recovery (FLR).....	366
	Recovering deduplication data.....	367
	Recovering with BMR.....	367
	Recovering ACL files.....	367
	Recovering encrypted data.....	367
	Recovering Windows volume mount points.....	368
	Recovering mount points.....	368
	Recovering nested mount points.....	368
	Recovering special Windows databases.....	369
	Recovering Windows DHCP and WINS databases.....	369
	Recovering expired save sets.....	369
	Recovering a recyclable or recoverable save set entry in the online indexes.....	370
	Recovering client files on a different NetWorker server.....	374
	Recovering critical NetWorker server databases.....	376
	Prerequisites to recover the NetWorker server databases.....	377
	Consider your recovery options.....	379
	Recovering the NetWorker server databases.....	379
	Options for running the nsrdr command.....	384
	Setting nsrdr tuning parameters.....	386
	Recovering the NMC server database.....	387
<b>Chapter 15</b>	<b>Enterprise reporting and events monitoring</b>	<b>389</b>
	Enterprise data reporting.....	390
	Enabling or Disabling the gathering of report data.....	390
	Data retention and expiration policies.....	391
	Setting expiration policies for data retention.....	392
	Report categories.....	392
	Report types.....	393
	How to configure reports.....	395
	How to view reports.....	398
	Preconfigured reports.....	404
	Customizing and saving reports.....	418
	Sharing reports.....	419
	Exporting reports.....	420
	Command line reporting.....	421
	Printing reports.....	423
	Enterprise events monitoring.....	423

About Events.....	423
Polling for System Events.....	424
Enabling or disabling the Capture Events option.....	424
Event viewing.....	424
Event priorities.....	425
Working with notes.....	426
Working with annotations.....	426
<b>Chapter 16      NetWorker server events reporting and monitoring</b>	<b>429</b>
Monitoring NetWorker server activities.....	430
About the Monitoring window.....	430
Groups window.....	432
Clones window.....	434
Sessions window.....	435
Alerts window.....	436
Devices window.....	437
Operations window.....	438
Log window.....	440
Archive Requests window.....	440
Recover window.....	442
Notifications.....	445
Preconfigured notifications.....	446
Customizing notifications.....	450
Logging event notifications.....	455
Creating a custom notification.....	456
Editing a notification.....	456
Copying a notification.....	456
Deleting a custom notification.....	457
Configuring owner notifications.....	457
Reporting group status and backup job status.....	458
Savegroup completion and failure notifications.....	458
Querying the job status.....	461
Reporting recover job status.....	464
Using nsrecomp.....	464
<b>Chapter 17      NMC Server Management</b>	<b>467</b>
NMC server authentication.....	468
Moving the NMC server.....	468
Setting system options to improve NMC server performance.....	470
Individual User Authentication.....	472
Setting environment variables.....	473
Setting environment variables on UNIX.....	473
Setting environment variables on Windows systems.....	474
Using the NMC Configuration Wizard.....	474
NetWorker NMC server maintenance tasks.....	474
Changing the service port used by the NetWorker Console database.....	474
Changing database connection credentials.....	475
Updating the NMC server IP address/hostname.....	476
Displaying international fonts in non-US locale environments.....	477
NetWorker License Manager.....	477
Entering an enabler code.....	477
Deleting an enabler code.....	477
Entering an authorization code.....	477

	Changing the License Manager server.....	478
<b>Chapter 18</b>	<b>NetWorker Server Management</b>	<b>479</b>
	Enterprise.....	480
	Enterprise components.....	480
	Organizing NetWorker servers.....	480
	Viewing the enterprise.....	481
	Managing various servers in the enterprise.....	481
	Managing folders in the enterprise.....	483
	Adding or deleting multiple servers by using a hostname file.....	485
	Setting up the server.....	487
	Hostname changes.....	487
	Report home.....	488
	Enabling the report home feature.....	488
	Manually running a report home report.....	489
	Disabling the report home feature.....	489
	Specifying additional email recipients for the report home report.....	489
	Specifying the sender email address.....	490
	Parallelism and multiplexing.....	490
	Parallelism.....	490
	Multiplexing.....	493
	Managing server access.....	494
	Working with the Multi-Tenancy Facility.....	494
	Users within a restricted data zone.....	495
	Create reports for a Restricted Data Zone.....	498
	View data within a Restricted Data Zone.....	498
	Restricted Data Zone resource associations.....	499
	Configuring a restricted data zone.....	499
	Configurations for the Multi-Tenancy feature.....	508
	Resource databases .....	509
	Viewing resources in the resource database.....	509
	Repairing resource database corruption.....	510
	Indexes.....	510
	Characteristics of the online indexes.....	510
	Automated index activities.....	511
	Checking online indexes.....	511
	Viewing information about the indexes.....	512
	Index save sets.....	512
	Querying the media database.....	513
	Cross-checking client file indexes.....	513
	Refreshing index information.....	514
	Client file index locations.....	514
	Changing the client file index location for an existing client.....	514
	Managing the size of the online indexes.....	515
	Managing Client Push.....	519
	Changing the location of the software repository.....	519
	Removing software package information from the software repository .....	520
	Transferring files and folders by using nsrpush.....	521
	Monitoring changes to the NetWorker and NMC Server resources.....	523
	Disabling or enabling the Monitor RAP Attribute.....	523
	Log file size management.....	523
	Internationalization.....	523
	Log file viewer.....	524
	Display issues.....	524

	Maximum path and save set length.....	524
	Locale-specific configuration issues on UNIX/Linux.....	525
	Server communication issues within Microsoft Windows.....	525
	Name resolution.....	526
	Backup Operators group.....	526
	Dynamic Host Configuration Protocol.....	526
	Backup and Recover Server service.....	526
<b>Chapter 19</b>	<b>NetWorker Client Management</b>	<b>527</b>
	NetWorker client overview.....	528
	Client configuration.....	528
	Creating a client.....	528
	Editing a client.....	528
	Copying a client.....	528
	Changing a client name.....	529
	Deleting a client.....	529
	Recreating a deleted client.....	530
	Hostname changes.....	530
	Editing a client NSRLA database.....	530
	Create a lockbox to store and retrieve pass phrases securely.....	531
	NetWorker authentication.....	531
	Creating multiple client resources for the same host.....	531
	Redefining a large file system backup into multiple client and save set instances.....	532
	Defining a client and save set combination.....	532
	Scheduled backups of non-ASCII files or directories.....	532
	Controlling access to a NetWorker client.....	533
	Client priority.....	533
	Dedicated client/server interface for backup and recovery operations.....	534
<b>Chapter 20</b>	<b>Block Based Backup and Recovery</b>	<b>535</b>
	Overview.....	536
	Supported operating systems and configurations.....	537
	Limitations.....	538
	Preparing for block based backups.....	538
	Creating a backup device.....	538
	Configuring block based backups.....	540
	Creating a CIFS share for block based recoveries-Optional.....	540
	Performing block based backups.....	541
	Scheduled backups.....	541
	Incremental backups.....	541
	Virtual full backups.....	542
	Synthetic full and incremental synthetic full backups.....	542
	Manual backups or client-initiated backups.....	542
	Save set backups.....	542
	Exclude list backups.....	543
	Windows deduplication volume backups.....	543
	CSV backups.....	543
	Windows BMR backups.....	543
	Verifying block based backups.....	543
	Cloning block based backups.....	544
	Performing block based recoveries.....	544
	Preparing for block based recoveries.....	544
	Using NMC to perform block based recoveries.....	544

	Using the CLI to perform block based recoveries.....	545
	Performing Windows BMR.....	547
	Performing block based clone recoveries.....	547
	Recovering data from Client Direct enabled devices.....	547
	Recovering data from Client Direct disabled devices.....	547
	Troubleshooting block based backup and recovery issues.....	549
<b>Chapter 21</b>	<b>NetWorker support for NDMP</b>	<b>551</b>
	Overview of NDMP.....	552
	Components in a NetWorker NDMP environment.....	552
	Configurations in a NetWorker NDMP environment.....	552
	NDMP local backup.....	553
	NDMP backups to non-NDMP devices (NDMP-DSA).....	554
	Three-party backup with NDMP devices.....	556
	Pre-configuration requirements for NDMP data operations.....	557
	NDMP feature requirements.....	557
	Locale requirements with NDMP.....	559
	Memory and space requirements for NDMP FH updates.....	560
	Performance Considerations.....	560
	NDMP licensing requirements.....	560
	Configuring Devices for NDMP operations.....	560
	NDMP device limitations.....	560
	DinoStor-managed jukeboxes.....	561
	Configuring NDMP on Isilon filer.....	561
	Determining NDMP device path names.....	561
	Configuring NDMP devices.....	563
	Configuring NDMP-DSA devices.....	567
	Configuring the Clone Storage Node.....	567
	Creating resources to support NDMP clients.....	568
	Creating and configuring the NDMP client resource.....	569
	Using the Client Configuration wizard.....	569
	Configuring the NDMP client manually.....	578
	Performing NDMP backups.....	578
	Performing an NDMP backup from the command line.....	579
	Troubleshooting NDMP configuration and backup failures.....	580
	Unable to connect to NDMP host hostname.....	580
	NetWorker features not supported on NetApp NDMP v3 and earlier.....	581
	Cannot perform NDMP backup after the NetWorker server licenses expire.....	581
	No PAX threads available.....	581
	Failed to store index entries.....	582
	IO_WritePage write failed - No space left on device (28): No space left on device.....	582
	Error reading the FH entries from save through stdin.....	582
	Cannot find file history info for filename...You may still be able to recover this file with a saveset recovery.....	582
	nsrndmp_save: data connect: failed to establish connection.....	583
	nsrndmp_save: get extension list: communication failure.....	583
	Cloning NDMP save sets.....	584
	Reporting NDMP Data.....	585
	Querying the NDMP volumes by backup type with the mminfo command.....	585
	Querying the NDMP save sets with the mminfo command.....	585
	Performing NDMP recoveries.....	586

	NDMP recovery requirements .....	587
	Performing an NDMP index-based file-by-file data recovery.....	589
	Performing a full or Directory Restore of NDMP data by using a save set recovery.....	592
	Performing destructive save set recoveries for vbb backups.....	595
	Troubleshooting NDMP recover.....	595
	RESTORE: could not create path pathname.....	596
	These files were not restored (Restore failed with error, or file/ directory specified but not found in backup) .....	596
<b>Chapter 22</b>	<b>SNMP Module</b>	<b>597</b>
	SNMP traps.....	598
	Configuring NetWorker SNMP notifications.....	598
	Command line options for nsrtrap.....	598
	Modifying preconfigured NetWorker SNMP notification.....	599
	Creating NetWorker SNMP notifications.....	600
	Configuring SNMP management software.....	600
	NetWorker SMI Network Management Private Enterprise Code.....	600
	Receiving traps in the SNMP network management software.....	600
<b>Chapter 23</b>	<b>DiskXtender Data Manager File System Support</b>	<b>603</b>
	Supported configurations.....	604
	Path information.....	604
	Permissions.....	604
	DiskXtender Data Manager file system overview.....	604
	File data in a DXDM file system.....	604
	Backup of DXDM file systems.....	606
	Excluding the DMAPI attributes file.....	606
	Aborted backups.....	607
	Recovery of DXDM file systems.....	608
	About recoveries.....	608
	Restoring deleted files and previous file versions.....	608
	File system synchronization.....	609
	Automatic synchronization.....	609
	Manually synchronizing a file.....	610
<b>Chapter 24</b>	<b>Windows Bare Metal Recovery</b>	<b>611</b>
	Terminology.....	612
	Overview of Windows Bare Metal Recovery (BMR).....	613
	Critical volumes.....	615
	WINDOWS ROLES AND FEATURES save set.....	616
	UEFI Partition Support.....	617
	Windows Server 2012 Cluster Shared Volumes (CSV) .....	617
	Windows Server 2012 Storage Spaces.....	618
	Online recovery of Active Directory, DFSR, or Cluster services .....	619
	Windows BMR Planning.....	620
	Hardware Requirements for Windows BMR backup and restore.....	620
	Save set configuration by host type.....	621
	Best Practices for Windows BMR.....	621
	Windows BMR limitations and considerations.....	622
	Performing a Windows BMR backup.....	628
	Including Windows BMR in scheduled backups.....	628
	Including Windows BMR in manual backups.....	630

	Verifying a valid Windows BMR backup .....	630
	Performing a Windows BMR recovery to physical or virtual computers.....	632
	Gathering configuration information required by a Windows BMR recovery.....	632
	Obtaining the Windows BMR image .....	632
	Creating a Windows BMR bootable image.....	634
	Performing a Windows BMR recovery to a physical computer.....	635
	Performing a BMR from a Physical Computer to a Virtual Machine (P2V) .....	641
	Troubleshooting Windows BMR.....	643
	Additional recovery options.....	647
	Reboot Required after Recovery Operation.....	648
<b>Chapter 25</b>	<b>Volume Shadow Copy Service</b>	<b>649</b>
	Overview of VSS.....	650
	VSS and the backup process.....	650
	Provider support.....	652
	The importance of writers .....	652
	Controlling VSS from NetWorker software.....	653
	Controlling VSS from the Administration window.....	653
	Control VSS from the command-prompt.....	654
	Globally disabling VSS.....	654
	VSS commands.....	655
<b>Chapter 26</b>	<b>Networking and connectivity</b>	<b>657</b>
	Name resolution and connectivity.....	658
	Troubleshooting name resolution and connectivity errors.....	658
	Verifying basic connectivity.....	659
	Verifying name resolution.....	661
	Verifying the NetWorker configuration.....	665
	Using multihomed systems.....	666
	Multihomed system requirements.....	667
	Configuring multihomed hosts in a datazone.....	667
	NIC Teaming.....	672
	Using DHCP clients.....	673
<b>Chapter 27</b>	<b>Troubleshooting</b>	<b>675</b>
	Before you contact technical support.....	676
	Determining the version of NetWorker software running on a client .....	676
	Displaying diagnostic mode attributes.....	677
	Viewing log files.....	677
	Locating savegroup job logs.....	678
	NetWorker functionality issues.....	679
	Backup and recovery.....	679
	Backups fail to start when the daylight savings time change occurs .....	680
	Shut down NetWorker services prior to any significant changes to system date.....	681
	Clone ID timestamp does not reflect the time the clone was created .....	681
	Backups fail to stop.....	681
	Memory usage when browsing large save sets.....	681

Memory usage and nsrjobd.....	682
Media position errors encountered when auto media verify is enabled .....	682
The scanner program marks a volume read-only.....	682
The scanner program requests an entry for record size .....	682
Limitations for groups containing a bootstrap.....	683
Index recovery to a different location fails .....	683
Illegal characters in configurations.....	683
Error backing up large number of clients.....	683
Hostname aliases.....	684
Directory pathname restrictions .....	684
Backup of a new client defaults to level full.....	684
Non-full backup of Solaris files with modified extended attributes.	685
Client file index errors.....	685
Cannot use the Console interface to stop the savegrp command....	686
Aborting a recovery .....	686
xdr of win32 attributes failed for directory.....	686
Cannot create directory directory.....	687
The All save set and duplicate drive serial numbers.....	687
No disk label errors.....	687
Cannot print bootstrap information.....	687
Server index not forced.....	687
Resolving copy violation errors.....	687
Converting sparse files to fully allocated files.....	688
Backing up large sparse files.....	688
Queries using the mminfo -N command are case-sensitive.....	689
Renamed directories and incremental backups.....	689
Resolving names for multiple network interface cards.....	689
Libraries entering ready state.....	690
Successful save sets listed as failed in the Group Backup Details window.....	690
The NetWorker Server window does not appear on HP-UX.....	690
Devices and Autochangers.....	690
Additional attributes in the Autochanger resource.....	690
Maintenance commands.....	691
Autodetected SCSI jukebox option causes server to stop responding .....	691
Autochanger inventory problems.....	691
Destination component full messages.....	691
Tapes do not fill to capacity.....	692
Tapes get stuck in drive when labeling tapes on Linux Red Hat platform.....	692
Increasing the value of Save Mount Time-out for label operations..	693
Server cannot access autochanger control port.....	693
Changing the sleep times required for TZ89 drive types .....	694
Message displayed when CDI enabled on NDMP or file type device .....	695
Verify firmware for switches and routers.....	695
Commands issued with nsrb on a multi-NIC host fail.....	695
SCSI reserve/release with dynamic drive sharing.....	695
Recovering save sets from a VTL on a different NetWorker server....	696
NetWorker locale and code set support.....	697
Enabling service mode for NetWorker.....	697
Network and server communication errors.....	697
Unapproved server error.....	697
Unapproved server error during client setup.....	698

	Server copy violation.....	698
	Remote recover access rights.....	698
	Authentication fails due to duplicate host names.....	699
	NetWorker server takes a long time to restart.....	699
	Changing the NetWorker server address.....	699
	Binding to server errors.....	700
	New.Net and NetWorker software are incompatible.....	700
	NetWorker archiving and retrieval.....	700
	Remote archive request from server fails.....	701
	Multiple save sets appear as a single archive save set.....	701
	Wrong archive pool is selected.....	701
	Second archive request does not execute.....	701
	The nsrarchive program does not start immediately.....	701
	Archive request succeeds but generates error when nsreexecd is not running.....	701
	Storage nodes.....	701
	Storage node affinity errors.....	702
	Storage node timeout errors.....	702
	Console error messages and corrective actions.....	703
	NMC log files.....	706
	The install log.....	707
	The gstd log.....	707
	Console troubleshooting notes and tips.....	707
	Troubleshooting an NMC server that is not responding.....	707
	Unable to connect to host: Please check Security setting and daemon logs on the Networker client and Console server for more details... 708	
	Username/password validation fails when you use the NMC New Device wizard to configure an AFTD if storage node is UNIX.....	709
	Querying large numbers of save sets in the NetWorker user interface may cause a Java heap space error.....	710
	NMC user interface exits unexpectedly.....	710
<b>Appendix A</b>	<b>Backing Up and Restoring a Microsoft DFS</b>	<b>711</b>
	Overview of a Microsoft DFS.....	712
	Domain-based DFS.....	712
	Registry-based DFS.....	712
	DFSR.....	712
	DFS junctions.....	712
	Save Set ALL-DFSR.....	712
	DFS topology information.....	713
	Configuring a scheduled DFS backup.....	713
	Restoring a DFS.....	714
	Authoritative restores of DFS Replication writers.....	714
	Non-authoritative DFS Replication writer granular recovery.....	714
<b>Appendix B</b>	<b>Additional Features of the Microsoft Windows Server</b>	<b>717</b>
	NetWorker Module for Microsoft.....	718
	Active Directory.....	718
	Active Directory backups.....	718
	Active Directory recoveries.....	718
	Encrypting file system.....	718
	Event logs.....	719
	Internet Information Server.....	719
	Windows registry.....	720

Sparse files.....	720
Advanced Configuration and Power Interface.....	720
Considerations for ACPI usage.....	720
Windows print queues.....	720
Windows Optimized Deduplication.....	721
Detecting Deduplication in a Backup.....	721
Data Deduplication Backup and Restore.....	721
Windows Data Deduplication Volume Best Practices.....	723
Recommended Deduplication Workloads.....	724
<b>Appendix C     UNIX and Linux Platform-Specific Notes</b>	<b>725</b>
Solaris.....	726
Solaris zone support.....	726
NetWorker executables not found for Solaris client.....	726
Support for tape devices not supported by Solaris.....	726
Extended file attribute data included in Save Set File Size attribute .....	726
The inquire command and Solaris 10.....	727
Improper font size for the Client Wizard with Netscape on Solaris.....	727
Linux.....	727
Backup considerations for Linux raw disk partitions .....	727
Configure Linux operating system to detect SCSI devices.....	727
The inquire command and the Scan for Devices operation do not detect more than 128 tape devices.....	727
Configuration requirements for the inquire command.....	728
Linux Journaled file system support.....	728
HP-UX.....	728
Autochanger installation on an HP-UX system.....	728
Errors from unsupported media in HP tape drives.....	731
Unloading tape drives on an HP-UX server or storage node.....	731
SCSI pass-through driver required for HP-UX autochangers.....	731
Symbolic link entries in the fstab file.....	732
Customized backup scripts.....	732
AIX.....	732
STK-9840 drives attached to AIX.....	732
LUS driver operation on AIX.....	732
Group ownership recovery.....	732
<b>Appendix D     OS-X Support</b>	<b>733</b>
Support for OS-X.....	734
OS-X metadata support.....	734
Supported file systems.....	734
OS-X backup considerations.....	734
Scheduling a NetWorker client backup on OS-X.....	734
Performing a manual backup on OS-X.....	736
Recovering files and directories from the command prompt.....	736
Recovering files and directories by using the NetWorker Recover GUI.....	737
Connecting to the NetWorker server.....	737
Changing the source NetWorker Client.....	738
Changing the browse time.....	739
Selecting objects to recover and recovering the data.....	739
<b>Appendix E     Direct SCSI Backup and Recover</b>	<b>743</b>

## CONTENTS

Introduction to direct SCSI backup and recover.....	744
System requirements.....	744
Unsupported features.....	744
About direct SCSI backups.....	745
Backing up data on a Symmetrix BCV device.....	745
Backing up data on a raw device.....	746
Backing up data from the command line.....	747
About direct SCSI recovers.....	747
Recovering data to a Symmetrix BCV device.....	748
Recovering data to a raw device.....	749
Licensing Direct SCSI.....	750
<b>Glossary</b>	<b>751</b>
<b>Index</b>	<b>767</b>

# FIGURES

1	NetWorker components .....	34
2	Console window.....	38
3	Administration window.....	39
4	NetWorker User program.....	45
5	Example of the browse window.....	47
6	Synthetic full backups.....	75
7	Save Sets query in NMC.....	88
8	How library sharing works.....	139
9	Example NetWorker DiskBackup configuration in a mixed backup environment.....	153
10	Example name and CIFS access information.....	166
11	Dynamic Drive Sharing.....	192
12	DDS with NDMP.....	195
13	One-week browse policy.....	233
14	Two-week browse policy.....	233
15	One-week backup cycle and three-week retention policy.....	235
16	Data lifecycle in the client index and the media database.....	236
17	How NetWorker groups are used to back up multiple clients.....	245
18	Weekly backup cycle.....	258
19	Default schedule for multiple clients.....	259
20	Staggered weekly schedules for multiple clients.....	259
21	Weekly synthetic full backup cycle to reduce backup window.....	260
22	Backups for October 1 through October 7 .....	265
23	Backups for October 1 through October 14.....	265
24	Backups for October 1 through October 15 .....	266
25	Using media pool configurations to sort data .....	286
26	Identifying WORM tapes in the NetWorker Console.....	295
27	Labeling a volume by using a label template.....	298
28	Overview of archive operation.....	307
29	A directed recovery from a remote client.....	349
30	Selecting a NetWorker Managed Application.....	430
31	Monitoring window.....	431
32	Recovery Window.....	443
33	NetWorker servers worldwide.....	481
34	NDMP local backup configuration .....	554
35	Backup initiated from a NetWorker server with an attached storage device.....	555
36	NDMP backup that uses immediate save.....	555
37	Three-party NDMP backup to NDMP devices.....	557
38	Prototypical DXDM installation.....	605
39	VSS backup process.....	651
40	Multihomed environment.....	669
41	Configuring the Aliases attribute for NetWorker server Client resource.....	670
42	Configuring the Aliases attribute for NetWorker storage node Client resource.....	670
43	Storage nodes attribute for clients in VLAN1 .....	671
44	Aliases and Server network interface attributes for VLAN1 clients .....	671
45	Storage node attribute for clients in VLAN2 .....	672
46	Aliases and Server network interface attributes for VLAN2 clients .....	672
47	Connect to Server .....	737
48	NetWorker Recover window .....	738
49	List of clients available for a NetWorker server.....	739
50	Search browse view.....	740
51	Versions side bar.....	741

## FIGURES

# TABLES

1	Revision history.....	29
2	Windows opened from the Console window .....	38
3	Windows launched from the Administration window.....	39
4	NetWorker User Groups requirements.....	46
5	NetWorker User toolbar functions .....	46
6	Services or programs on the NetWorker server .....	52
7	Services or programs on the NetWorker client.....	53
8	Services or programs on the NetWorker storage node .....	53
9	Services or programs on the NetWorker Management NMC server.....	54
10	NetWorker startup commands .....	56
11	Accounting department backup requirements.....	61
12	Components in the ALL save set .....	69
13	Special ALL save sets .....	70
14	Synthetic full backup levels.....	79
15	Traditional synthetic full and virtual synthetic full backups.....	85
16	mminfo command for VSF validation .....	87
17	PSS support in NetWorker.....	89
18	New Checkpoint Restart media attributes.....	100
19	Job Control selections.....	116
20	Common jbedit options.....	137
21	Library resource sleep attributes .....	139
22	Tape alert severity.....	144
23	StorageTek environment variables .....	149
24	Differences between disk devices .....	154
25	Default values and ranges for target and max sessions attributes .....	165
26	A comparison of cloud devices to other device types.....	174
27	Device settings and environment variables .....	184
28	Shared Devices attributes.....	196
29	Volumes detail .....	208
30	Volume modes .....	209
31	Group attributes .....	246
32	Probe group fields.....	248
33	savegrp options that are not taken from backup group resource attributes .....	252
34	Preconfigured NetWorker schedules .....	257
35	Key components of a schedule .....	261
36	Backup levels .....	264
37	Advantages and disadvantages of backup levels .....	266
38	Regular file and index backup levels .....	268
39	Preconfigured directives.....	274
40	Save environment keywords .....	277
41	NetWorker ASMs .....	278
42	Attributes to direct client indexes and bootstrap to a separate media pool .....	286
43	NetWorker hierarchy for resolving media pool conflicts .....	287
44	WORM supported devices .....	294
45	WORM/DLTWORM attributes .....	296
46	Key label template attributes.....	299
47	Examples of number sequences for volume labels.....	300
48	Using label template components.....	301
49	Save set status settings.....	326
50	List of nsrclone options and their descriptions.....	338
51	General recover requirements .....	349

52	Command line recovery considerations .....	358
53	Optional browsable recovery options .....	362
54	Optional save set recovery options .....	364
55	Command line options for the nsrdr command.....	384
56	Data retention policies.....	391
57	Report categories .....	392
58	Report icons.....	394
59	Date and time input formats for common locales.....	396
60	Report chart formats.....	401
61	NetWorker backup statistics parameters .....	405
62	NetWorker backup status parameters .....	407
63	Clone report parameters .....	408
64	NetWorker recovery statistics parameters .....	410
65	Avamar Statistics parameters .....	412
66	Event parameters .....	414
67	Host reports .....	415
68	Cloud backup and recover parameters .....	416
69	Report export formats.....	420
70	Events columns .....	425
71	Event priorities .....	425
72	Monitoring window panel .....	431
73	Groups window icons.....	433
74	Sessions that can be stopped from NMC .....	436
75	Alerts window icons.....	436
76	Devices window icons .....	437
77	Operations window icons.....	438
78	Log window icons .....	440
79	Archive requests window icons.....	441
80	Recovery toolbar options .....	443
81	Save recover configuration job status.....	444
82	Find options.....	445
83	Preconfigured notifications .....	446
84	Events .....	450
85	Actions .....	452
86	Priorities .....	455
87	Event Viewer messages .....	456
88	The recoverpsm options .....	469
89	NMC server system options .....	470
90	Console environment variables.....	473
91	Viewing the enterprise.....	481
92	Tenant administrator privileges.....	504
93	Indexes window information.....	512
94	Index save sets dialog box information.....	512
95	When to modify the servers file.....	533
96	Supported backup and recovery scenarios.....	537
97	Key options for the block based recover.exe command.....	546
98	Troubleshooting block based backup and recovery issues.....	549
99	Distinctions between NDMP Tape Server and NDMP-DSA .....	553
100	NDMP features.....	557
101	Determining NDMP path names.....	562
102	NDMP resource requirements.....	568
103	Supported backup types.....	570
104	Vendor-specific Application Information variables.....	571
105	Requirements of each NDMP recovery feature.....	587
106	Command-line options for nsrtrap .....	598
107	DXDM file system data types included in a NetWorker backup.....	606

108	DISASTER_RECOVERY:\ components in an incremental backup.....	614
109	Save set configuration for a specific host .....	621
110	Additional recovery options.....	647
111	VSS Save operation attribute values .....	655
112	Configuring multihomed hosts in NetWorker (continued).....	667
113	NetWorker Startup commands.....	700
114	Error messages or symptoms .....	703
115	Environment variables for the gstd.raw.....	707

## TABLES

# Preface

As part of an effort to improve its product lines, EMC periodically releases revisions of its software and hardware. Therefore, some functions 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 properly 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 describes how to configure and use EMC NetWorker.

## Audience

This guide is part of the NetWorker documentation set, and is intended for use by system administrators who are responsible for setting up and maintaining backups on a network. Operators who monitor daily backups will also find this guide useful.

## Revision history

The following table presents the revision history of this document.

**Table 1** Revision history

Revision	Date	Description
05	November 28, 2014	<ul style="list-style-type: none"><li>Provided list of cleaning attributes for TapeAlert feature</li><li>Corrected example of a skip directive to skip temporary files</li><li>Revised information in the section "Delaying tape device cleaning"</li></ul>
04	November 3, 2014	<ul style="list-style-type: none"><li>Clarified instructions for backup of Windows mapped drives</li><li>Restriction against Client Name for NAS or NDMP backups specified by Isilon SmartConnect or having aggregated connections</li></ul>
03	October 3, 2014	<ul style="list-style-type: none"><li>Revised table of contents</li></ul>
02	September 23, 2014	<ul style="list-style-type: none"><li>Document formatting changes</li></ul>
01	June 18, 2014	<ul style="list-style-type: none"><li>First release of this document for EMC NetWorker 8.2</li></ul>

## Related documentation

The NetWorker documentation set includes the following publications:

- *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 [support.emc.com](http://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 Cluster Installation 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 Avamar Devices Integration Guide*  
Provides planning and configuration information on the use of Avamar devices in a NetWorker environment.
- *EMC NetWorker Command Reference Guide*  
Provides reference information for NetWorker commands and options.
- *EMC NetWorker Data Domain Deduplication Devices 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 Error Message Guide*  
Provides information on common NetWorker error messages.
- *EMC NetWorker Licensing Guide*  
Provides information about licensing NetWorker products and features.
- *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 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 used in this document

EMC uses the following conventions for special notices:

##### **NOTICE**

Addresses practices not related to personal injury.

---

##### **Note**

Presents information that is important, but not hazard-related.

## Typographical conventions

EMC uses the following type style conventions in this document:

<i>Italic</i>	Use for full titles of publications referenced in text
Monospace	Use for:
	<ul style="list-style-type: none"> <li>• System code</li> <li>• System output, such as an error message or script</li> <li>• Pathnames, file names, prompts, and syntax</li> <li>• Commands and options</li> </ul>
<i>Monospace italic</i>	Use for variables
<b>Monospace bold</b>	Use 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 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. You will see several options for contacting EMC Technical Support. 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

Visit 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 will help us continue to improve the accuracy, organization, and overall quality of the user publications. Send your opinions of this document to [DPAD.Doc.Feedback@emc.com](mailto:DPAD.Doc.Feedback@emc.com)



# CHAPTER 1

## Overview

This chapter contains the following topics:

- [The NetWorker environment](#)..... 34
- [NetWorker features](#)..... 35
- [NetWorker user interfaces](#)..... 37
- [Common NetWorker tasks](#)..... 48
- [NetWorker services](#)..... 52

# The NetWorker environment

The ®NetWorker® environment provides the ability to protect an enterprise against data loss. As the enterprise grows, so does the complexity and importance of protecting data. NetWorker software provides the power and flexibility to meet these challenges.

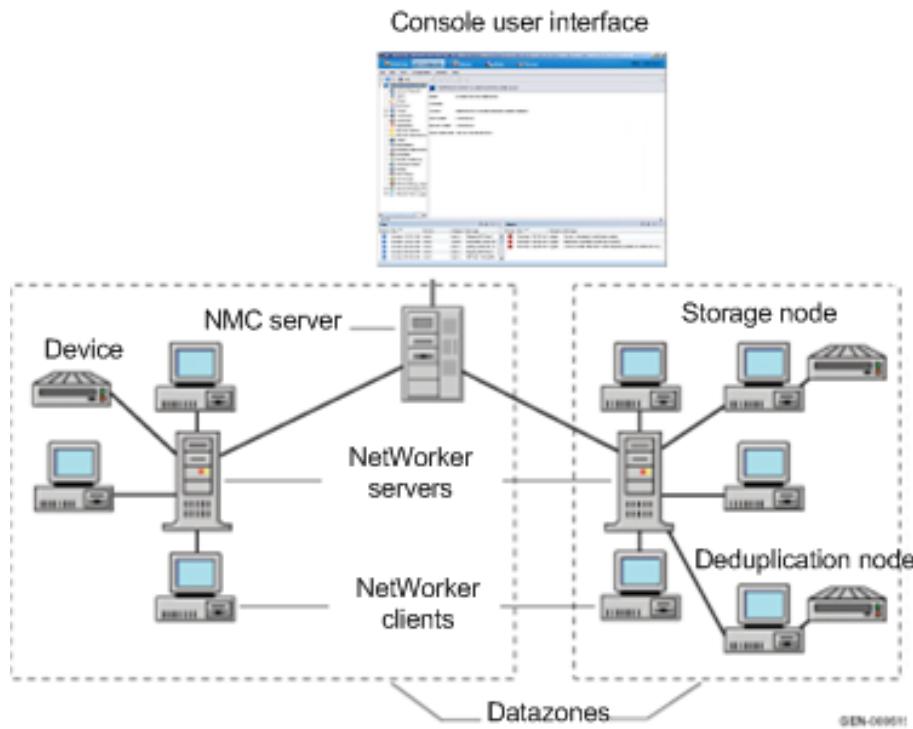
The NetWorker software is a cross-platform, client/server application that provides the ability to remotely manage all NetWorker clients and servers from a web-enabled, graphical interface.

## NetWorker components

There are several components that make up the NetWorker environment and provide the ability to protect against data loss.

The following figure illustrates the main components in a NetWorker environment.

**Figure 1** NetWorker components



### NMC server

The NetWorker Management Console (NMC) server manages all NetWorker servers and clients. The NMC server also provides reporting and monitoring capabilities for all NetWorker servers and clients in your environment.

### Console user interface

The NMC server uses a graphical interface that runs from any computer in your environment that has a supported web browser and Java Runtime Environment (JRE). The NetWorker Installation Guide provides information on supported web browsers and supported versions of the JRE. Multiple users can access the NMC server concurrently.

from different browser sessions. A computer that hosts the web browser can also be a NetWorker client.

## Datazone

A datazone is a single NetWorker server and its client computers. Datazones can be added as backup requirements increase.

## NetWorker server

NetWorker servers provide services to back up and recover data on NetWorker client computers in a datazone.

## NetWorker client

A NetWorker client computer is any computer in a datazone with data that must be backed up. The NetWorker NMC server, NetWorker servers, and NetWorker storage nodes are also NetWorker clients.

## NetWorker storage node

A NetWorker storage node can be used to improve performance by offloading from the NetWorker server much of the data movement involved in a backup or recovery operation.

## Deduplication storage systems

The NetWorker software supports backup data deduplication on EMC Avamar® storage nodes and on Data Domain® storage systems.

The *EMC NetWorker Avamar Integration Guide*, provides detailed information about setting up Avamar deduplication to work with NetWorker.

The *EMC NetWorker Data Domain Deduplication Devices Integration Guide* provides detailed information about setting up DD Boost deduplication devices to work with NetWorker.

## Virtual environments

NetWorker clients can be created for virtual machines for either traditional backup or VMware Consolidated Backup (VCB). Additionally, the NetWorker software can automatically discover virtual environments and changes to those environments on either a scheduled or on-demand basis and provides a graphical view of those environments.

# NetWorker features

The NetWorker software has many features and functionality that optimize it for high-speed backup and recovery operations of large amounts of complex data across entire datazones.

This section describes the major features that distinguish the NetWorker software. Optional additions to the NetWorker software are also listed.

## Performance features

There are several standard NetWorker performance features that can be configured to enhance performance in any environment.

NetWorker performance features include:

- Server parallelism, which enables several *save streams* to flow to the server or storage node at the same time.
- Multiplexing, which enables more than one save stream to write to the same device at the same time.
- Client parallelism, which enables the client to send more than one save stream at a time.
- Client Direct, which enables client backups to bypass the storage node and send deduplicated backup data directly to DD Boost storage devices, or to send non-deduplicated backup data directly to AFTD storage.
- Session management, which enables control of the number of save streams per device to maximize device performance.
- Backup to file-based devices and optional subsequent staging and cloning to near-line or offline volumes.
- Backup to a cloud storage configuration.

## Ease of use

NetWorker software provides tools to make protection of critical data easy to manage. With these tools, you can:

- Use either the graphical interfaces or command-line programs to manage NetWorker tasks and functions.
- Use wizards to set up the following NetWorker items:
  - Client resources
  - AFTD and Data Domain devices
  - Common Console configuration tasks
  - LDAP user authentication
- Administer and configure NetWorker functions from any network computer with a web browser.
- Grant permission to provide directed recovery operations. Directed recovery is the capability to recover of data from one client computer to another client computer.
- Obtain immediate answers to questions by accessing online help and UNIX man pages. Microsoft Windows users can also access the NetWorker command reference guide, which provides information similar to the UNIX man pages.
- Take advantage of the automatic media management feature to enable the NetWorker server or storage node to label and mount volumes as needed for backups.
- Drag-and-drop functionality allows for the easy transfer of single or multiple objects.
- Use the integrated knowledge base and technical notes at the EMC Online Support® website to find answers to common questions.
- Automatically discover and view a graphical map of virtual environments.
- Set up NetWorker NMC server authentication to an external LDAP v3 compliant server. The *EMC NetWorker Security Configuration Guide* describes how to configure the NMC server to use LDAP authentication.
- Support for automated Windows Bare Metal recovery.

## Scalability

NetWorker software can be scaled as storage management needs grow.

For example, you can:

- Upgrade the basic level of server functionality, add support for additional (or larger) autochangers, add support for more clients, or add optional software modules without the need to reinstall the server software.
- Add special NetWorker Module client software to back up databases and other non-file-system data.
- Add support for remote storage nodes to control backup devices, while the data management tasks remain centralized on a controlling NetWorker server.
- Add the NetWorker License Manager (NLM) software to administer all EMC software licenses from a single server.

## Optional software additions

There are many optional additions to the NetWorker software that further enhance performance and functionality.

Optional features include:

- NetWorker Autochanger Module
- NetWorker Silo Software Module
- NetWorker Archive Module
- NetWorker Database Modules (for the back up and recovery of supported database applications)
- NetWorker SNMP (Simple Network Management Protocol)
- NDMP (Network Data Management Protocol) support
- Cluster support
- NetWorker License Manager
- Advanced reporting capability

## NetWorker user interfaces

The NetWorker application consists of several user interfaces that provide the ability to configure and use NetWorker features and functionality.

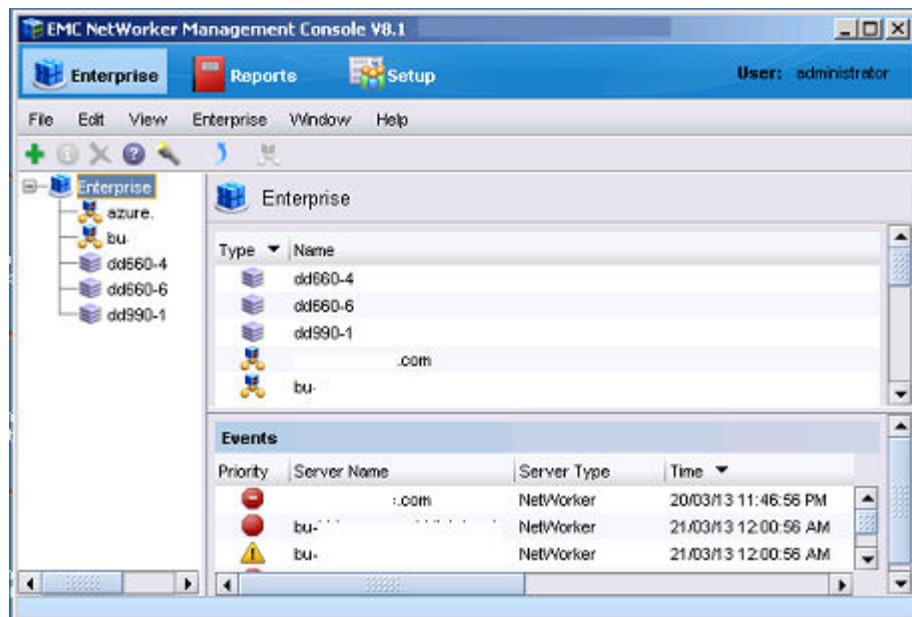
### NetWorker Management Console interface

The interface for NetWorker Management Console (NMC), also called the NetWorker Console, consists of both the Console window, and the Administration window.

#### Console window

When NetWorker software is started, the Console window opens.

The following figure illustrates the Console window.

**Figure 2** Console window

The Console window is the first point of access for NetWorker tasks. The following table lists the task-based windows that can be opened from the Console window toolbar.

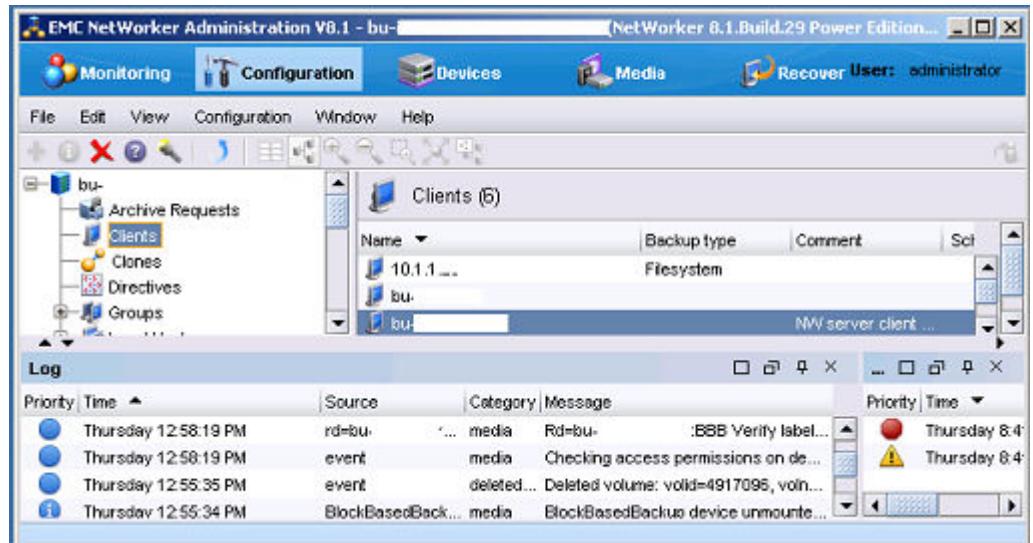
**Table 2** Windows opened from the Console window

Button	Window	Description
	Enterprise	Select a NetWorker server to manage and monitor the server and its backup clients. The Enterprise window provides the ability to open the Administration window for a NetWorker server.
	Reports	Configure and view Console reports.
	Setup	Control administrative functions: <ul style="list-style-type: none"> <li>User management — Add, edit, and delete Console user accounts, restrict user views of servers. The <i>EMC NetWorker Security Configuration Guide</i> provides information about user management.</li> <li>License management — Manage NetWorker licenses. The new for 7.6 Service Pack 1 <i>EMC NetWorker Licensing Guide</i> provides information about license management.</li> </ul>
	Events	View important messages about all NetWorker servers that are added as Enterprise applications. This includes both the NMC server, and the Avamar server.

## Administration window

NetWorker servers are managed through the Administration window.

The following figure illustrates the NetWorker Administration window.

**Figure 3** Administration window

You can toggle between the Administration window and the Console window.

The following table lists the windows that can be launched from the Administration window toolbar.

**Table 3** Windows launched from the Administration window

Button	Window	Description
	Monitoring	Monitor various activities related to the NetWorker server. For example, you can monitor the progress of a scheduled backup and view any alerts. A portion of the Monitoring window appears at the bottom of the Administration window at all times, providing information on Log messages and Alerts.
	Configuration	Manage the NetWorker server and its resources such as clients, backup schedules, and policies. For example, you can create a backup schedule, add NetWorker clients, and apply the backup schedule to several NetWorker clients.
	Devices	Add, configure, and operate single or multiple devices, libraries, and silos for the NetWorker server.
	Media	Manage activities and resources related to backup volumes. For example, you can mount a backup volume or create a template for labeling backup volumes.
	Recover	Manage recover configurations and schedule recover jobs for NetWorker hosts from a centralized location on the NMC server.

## Starting the Console for the first time

These steps assume that the NetWorker software is installed and that all of the software and hardware requirements have been met on the computer that will access Console. The *EMC NetWorker Installation Guide* provides more information.

## Procedure

1. From a supported a web browser session, type the URL of the NMC server:

```
http://server_name:http_service_port
```

where:

- server\_name is the name of the NMC server.
- http\_service\_port is the port for the embedded HTTP server. The default HTTP port is 9000.

For example:

```
http://houston:9000
```

2. On the **Welcome** window, click **Start**.
3. On the **Security Warning** window, click **Start** to install and run **NetWorker Console**.
4. On the **Licensing Agreement** window, select **Accept**.
5. If you did not install the appropriate JRE version on the system, a prompt to install JRE appears. Follow the prompts to install JRE.
6. On the **Welcome to the Console Configuration Wizard** window, click **Next**.
7. On the **Set Administrator password** window, type the NMC password, then click **Next**.
8. On the **Set Database Backup Server** window, specify the name of the NetWorker server that will backup the NMC server database, and click **Next**.
9. On the **Add NetWorker servers** window, specify the names of the NetWorker server that the NMC server will manage, one name per line. Leave the default options **Capture Events** and **Gather Reporting Data** enabled.

Consider the following:

- The **Capture Events** option enables the NMC server to monitor and record alerts for events that occur on the NetWorker server.
- The **Gather Reporting Data** option enables the NMC server to automatically collect data about the NetWorker server and generate reports. The *EMC NetWorker Administration Guide* on the EMC Online Support site describes available reports and how to run them.

10. Click **Finish**.

The **Console** window and the **Getting Started** window open.

11. In the **Enterprise** window, right click the NetWorker server and select **Launch Application**.

## Starting the Console after the first time

You can restart the Console after it has been started the first time.

- Point the browser to the same URL.
- Double-click the NetWorker Console product name in the Java Web Start Application Manager.
- Double-click the desktop button, if one was configured by using the Java Web Start Application Manager.

## Opening the Administration Window

You can add and select a NetWorker server and open the Administration window.

### Procedure

1. From the **Console** window, click **Enterprise**.
2. Add one or more NetWorker servers:
  - a. Highlight **Enterprise** in the navigation tree.
  - b. From the **File** menu, select **New>Host**.
  - c. Type the name of the host on which the NetWorker server is running and click **Next**.
  - d. Select **NetWorker** for the type of application to be managed.
  - e. Click **Finish**.
  - f. Repeat for all NetWorker servers in your network.
3. From the left pane, click a host in the **Enterprise** list.
4. From the right pane, click the application and select **Enterprise > Launch Application**, or double-click the application. The **Administration** window opens as a separate application.

## Sorting tables

Console software's organization and display of tabular information can be changed. Table grids can be sorted by column heading, and then by alphabetic or numeric order within those columns.

### Procedure

1. Drag-and-drop the column heading to its new position.
2. Click the column heading to sort the items into alphabetic and numeric order. An arrow appears in the column heading to indicate the sort order.
3. John wants to see all the managed events about servers that were unreachable by the NMC server. Sorting managed events (Step example):
  - a. From the Console window, John clicks **Events**.
  - b. He clicks and drags the **Message** column until it is over the **Priority** column, where he drops it.
  - c. He clicks the **Message** column heading so that a down-arrow appears.

### Results

Now John can scan down the list of messages until he finds all three servers with the message, **Unable to connect to server**.

John can also generate a **Managed Event Details** report to get the same information, and then print, or export it for use in another application.

## Sorting selected rows in a table

Selected rows will be sorted to the top of the table. This is particularly useful when you select **Highlight All** from the Find panel to select all rows matching the Find criteria and then moving all selected rows to the top of the table to view the results.

### Procedure

1. From the **Edit** menu, select **Find** or press **Ctrl + F** to view the **Find** panel.

2. Click the rows to be selected or select rows by using the Find criteria.
3. Select **Sort Selected**.

## Sorting multiple columns in a table

For example, given a large table of events, you can select the Time column as the tertiary sort key, the Category column for the secondary sort key, and the Server name as the primary sort key. The resulting display would list the servers in alphabetical order, and the events for each server would be grouped by category and would display in chronological order.

### Procedure

1. Click the column to be used as the last sort key.
2. Click the column to be used as the next-to-last sort key and so on until the primary column is selected.

## Displaying columns in a table

You can select which columns to display in a table.

### Procedure

1. From the **View** menu, select **Choose Table Columns**.
2. Click a column name to select or clear the column and then click **OK**.

You can also select the columns to display by right-clicking on a table header and selecting **Add Column** from the drop-down.

## Editing multiple resources

In the NMC Configuration window, you can edit an attribute for multiple resources at the same time.

For example, if you want all clients within a group to have their backup schedule changed from the default to “Full Every Friday”, do the following:

### Procedure

1. Select each client resource row in the window.
  2. Place the cursor in the column you want to change (in this case, the Schedule column).
- The color of the column changes when the cursor is in the column.
3. Right-click in that column and select from the list of available options. The options include **Edit**, **Add to** and **Remove from**, depending on the column selected.

Only the columns that appear in the window can be selected for multiple resource editing. To add a column that is not currently in view:

- a. Right-click on a table header and select **Add Column** from the drop-down.
- b. Select from the list of available attributes.

## Drag-and-drop functionality

Drag-and-drop functionality is available in the Console and Administration interfaces for many tasks.

## Drag-and-drop between resource types in the Console window

The drag-and-drop functionality allows multiple resources to be selected and moved from one resource type to another.

In the Enterprise window from the Console interface, you can drag-and-drop to perform the following actions:

- Copy an individual folder in the enterprise hierarchy by selecting the folder, holding down the **Ctrl** key, and dragging the folder to a new location.
- Move an individual folder in the enterprise hierarchy to a new location by selecting and dragging a folder to a new location.
- Copy an individual host node in the enterprise hierarchy by selecting and dragging the host to a new parent folder.
- Move an individual host node in the enterprise hierarchy by selecting and dragging the host to a new parent folder.
- Copy a selected number of objects in a folder to a new folder in the hierarchy tree or folder contents table. Select an individual folder in the navigation tree to display the contents of the folder, select the contents, while pressing **Ctrl**, drag the contents to a new folder. Select a collection of folders and/or hosts and drag them to a new folder by creating a copy of the selected contents in a new location.
- Move a selected number of objects in a folder to a new folder in the hierarchy tree or folder contents table. Select an individual folder in the navigation tree to display the contents of the folder, select the contents and drag the contents to a new folder. Select a collection of folders and/or hosts and drag them to a new folder by moving the selected contents to a new location.

**NOTICE**

Only one object may be selected for drag-and-drop in the navigation tree.

---

## Client and group management in the Administration window

The drag-and-drop functionality allows multiple clients or groups to be selected and moved from one location to another. You can use drag-and-drop functionality in the Configuration window to do the following:

- Copy selected clients to a new NetWorker group:
  - Expand and select a group in the directory tree.
  - Drag-and-drop the client objects in the Client Summary table to a new group in the directory tree.
- Copy selected clients from one NetWorker group to a new group:
  - Select a group in the directory tree.
  - Move clients from the Client Summary table to another NetWorker group.
- Move selected clients to a new NetWorker group:
  - Expand a group in the directory tree and select one or more clients.
  - Drag-and-drop the client objects in the Client Summary table to a new group in the directory tree.

This removes the client objects from the initial NetWorker group.

- Change a current group schedule to a selected schedule:
  - Select a group in the directory tree to display the group objects.

- Drag-and-drop a schedule in the Schedule Summary table to a different group in the directory tree.

## Library operations in the Devices window

The drag-and-drop functionality allows multiple slots or devices to be managed in the Devices window.

You can use drag-and-drop functionality to manage media from the Library window from the Devices task, for instance:

- Mount an individual volume onto a device by selecting a slot in the Slots table and dragging it to a device in the Devices table.
- Mount multiple volumes to available devices as assigned by the NetWorker server. To mount multiple volumes, select multiple slots in the Slots table and drag them anywhere in the Devices table.
- Unmount a volume from a selected device and deposit it back in its designated slot by selecting an individual device from the Devices table and dragging it anywhere in the Slots table. The volume image displays in the corresponding slot.
- Unmount multiple volumes from a selected device and deposit them back in their designated slot by selecting the devices from the Devices table and dragging them anywhere in the Slots table. The volumes display in the corresponding slots.

## Copy and paste tabular information to operating system clipboard

Tabular information can be selected and moved to an operating system clipboard by using drag-and-drop functionality. All tables support selection of multiple rows in a table and the ability to copy and paste the data in the selected rows to the system clipboard. Subsequently, the data in the operating system clipboard can be moved to a target application.

### **NOTICE**

Drag-and-drop operations from the operating system clipboard to a table are not supported.

---

## Multiple library devices and slots

A single operation can be performed on multiple library devices and slots. Multiple rows can be selected in both the Devices and Slots tables simultaneously.

In the Devices table for a library, multiple devices can be selected to perform the following operations:

- Unmount
- Release device (STL only)
- Enable/Disable

In the Slots table for a device, multiple volume operations can be performed for the following operations:

- Mount
- Load without mount
- Withdraw
- Label
- Inventory
- Remove (STL and EMC AlphaStor® only)

## Setting user interaction preferences

Depending on the window button that was selected from the Console window, you can set various user preferences such as the user interface font, font size, parallel windows, and table settings. For the Reports window, there are ways you can enhance the viewing of displayed reports.

### Procedure

1. Select **View** on the main menu.
2. Set the various options available under the selected window button. You may need to click **OK**, depending on your option selection.

## NetWorker client interface

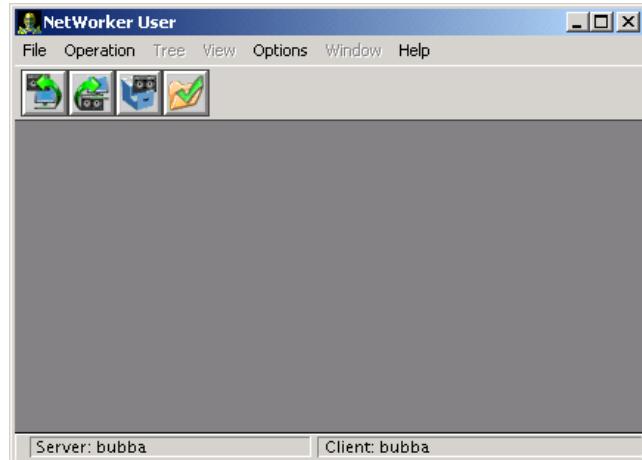
The client interface is where users can recover data and perform manual backup and archive operations. Manual operations are not scheduled. Instead, they are performed when a user wants to back up or archive one or more files on the NetWorker client immediately. Scheduled backup and archive operations are set up through the Console interface.

### Windows client interface

The NetWorker User program provides the ability to manage clients in the NetWorker environment.

The following figure illustrates the Windows client interface.

**Figure 4** NetWorker User program



## Starting the NetWorker User program on Windows

There are 2 ways to start the NetWorker User program.

- Click the Windows Start button and select Programs>EMC NetWorker>NetWorker User.
- From the Administration window, click Start on the main menu, select “NetWorker User...” If the NetWorker Module for Microsoft Applications is installed on the client computer, this operation starts the NetWorker Module for Microsoft Applications instead.

The NetWorker client package must be installed on the host where you start the NetWorker User program. Otherwise, you will see an error message similar to the following:

The user program you are trying to run (winworkr) is either not installed on this computer, or is not in your path.

To start the NetWorker User program, you must belong to the appropriate Windows groups. The following table lists the groups that you must belong to in order to run the NetWorker User program.

The Backup Operators and Administrators groups are the local and remote Microsoft security groups.

**Table 4** NetWorker User Groups requirements

Logged on	Workstation	Server	Server (domain controller only)
Locally	Backup Operators or Administrators	Backup Operators or Administrators	Not applicable
To the domain	Domain Administrators	Domain Administrators	Backup Operators or Administrators

## Toolbar buttons

The NetWorker User program has a toolbar with buttons for common User program tasks. The following table describes the function of each button.

**Table 5** NetWorker User toolbar functions

Button	Name	Function
	Backup	Starts a manual (unscheduled) backup of the client's data to a NetWorker server.
	Recover	Starts a recovery operation to retrieve copies of saved data back to the client computer.
	Archive	Starts an archive operation to save copies of data to a server for storage on an archive volume. Once the data is stored on the archive volume, you have the option of removing the data from the disk.
	Verify	Starts a verification operation to ensure that the data items just backed up are the same as those currently on the disk.

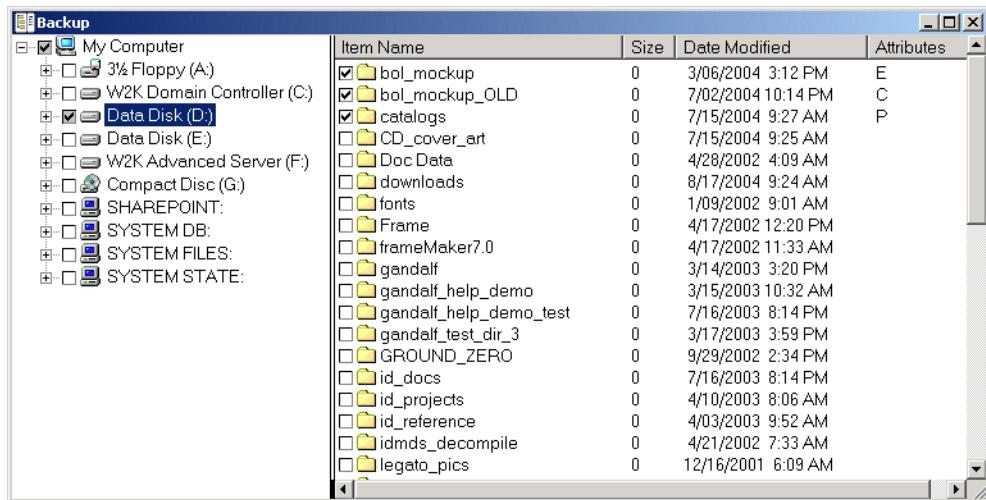
## Browse window

A browse window opens in the NetWorker User program if you select menu items or buttons.

A browse window opens if you select any of the following items:

- A toolbar button
- A Backup, Recover, Archive, Verify, or Local Directive command from the NetWorker User File menu

The browse window, shown in the following figure, displays the directory tree of the file system that is being browsed.

**Figure 5** Example of the browse window**NOTICE**

When you mark a disk volume or directory for an operation, all of its nested subdirectories and files are also marked.

A checkmark beside an item name indicates that the item is selected for backup, recovery, archiving, or verification.

The Attributes column indicates any special handling option that was applied:

- P — The item is marked for password-protection.
- E — The item is marked for password-protection and encryption, using the PW2 ASM.
- C — The item is marked for compression.

## Connecting to a NetWorker server

A typical user that runs the NetWorker User program needs to connect to the NetWorker server that performs scheduled backups. However, to perform a directed recovery or to back up files to another server, you might need to connect to a different NetWorker server.

Before the NetWorker User program can connect to a NetWorker server, the client computer must be set up as a Client resource on that NetWorker server:

### Procedure

1. From the **Operation** menu, select **Change NetWorker Server**.
2. In the **Change Server** dialog box, select a server from the list of available NetWorker servers. If the server is not listed, do one of the following:
  - Click **Update List** to search the network for available NetWorker servers.
  - Type the server's hostname.
3. Click **OK**.

## UNIX client interfaces

On UNIX, use command line utilities to perform manual backups (the save command), archiving (nsrarchive) and recovery operations (recover). For more information on these commands, refer to the *EMC NetWorker Command Reference Guide* or the UNIX man pages.

## NetWorker character-based interface

Use the NetWorker character-based interface (nsadmin) to perform configuration and management tasks for a NetWorker server.

You can start the nsadmin interface by using this command:

```
nsadmin
```

For more information about nsadmin, refer to the *EMC NetWorker Command Reference Guide* or the UNIX man pages.

## NetWorker command-line interface

Perform client and server tasks by typing commands at the prompt. The *EMC NetWorker Command Reference Guide* or the UNIX man pages provides information about these commands.

## Common NetWorker tasks

There are several common tasks available in the NetWorker Console.

### Adding a new host

You can add new hosts by using the NetWorker Console.

#### Procedure

1. Log in to Console as a NetWorker Administrator.
2. Click the **Enterprise** button  on the taskbar.
3. Right-click **Enterprise** in the navigation tree.
4. Select **New > Host**.
5. In the **Host Name** field, specify the IP address, DNS name, or WINS name of the NetWorker server and click **Next**.
6. In the **Select Host Type** window, select **NetWorker** and click **Next**.
7. In the **Manage NetWorker** window, leave the default options **Capture Events** and **Gather Reporting Data** enabled.
  - Enable the **Capture Events** option to allow the NMC server to monitor and record alerts for events that occur on the NetWorker server.
  - Enable the **Gather Reporting Data** option to allow the NMC server to automatically collect data about the NetWorker server and generate reports. The *EMC NetWorker Administration Guide* on the EMC Online Support Site describes on how to run reports and the reports that are available.
8. Click **Finish**.

### Device configuration

You can configure devices to test the NetWorker software.

Configure one of the following devices to test the NetWorker software:

- [Configuring a stand-alone tape device on page 49](#)

- [Configuring a stand-alone advanced file type device on page 49](#)
- [Configuring an autochanger or silo on page 49](#)

## Configuring a stand-alone tape device

### Procedure

1. Log in to the Console as a NetWorker Administrator.
2. Click the **Enterprise** button  on the taskbar.
3. Highlight a host in the navigation tree, right-click **NetWorker** and select **Launch Application**. The **NetWorker Administration** window appears.
4. Click the **Configuration** button  on the taskbar.
5. Click the **Devices** button  on the taskbar.
6. In the navigation tree view, right-click a host and select **Scan for Devices**.
7. From the right pane, select the new device.
8. From the **Devices** menu, select **Devices > Device Operations > Label**.
9. In the **Label** window, verify the information and click **OK**.

## Configuring a stand-alone advanced file type device

### Procedure

1. Log in to the Console as a NetWorker Administrator.
2. Click the **Enterprise** button  on the taskbar.
3. Highlight a host in the navigation tree, right-click **NetWorker** and select **Launch Application**. The **NetWorker Administration** window appears.
4. Click the **Configuration** button  on the taskbar.
5. Click the **Devices** button  on the taskbar.
6. In the **Select Device Type** window, select Advanced File Type Device (AFTD), then click **Next**.
7. From the **File** menu, select **New Device Wizard**.
8. In the **Select Storage Node** window, click **Next**.
9. In the **Select the Device Path** window, select an empty folder or create a new folder on the NetWorker server, then click **Next**.
10. In the **Configure Attributes** window, specify a name for the new device, for example: **myaftd**, then click **Next**.
11. In the **Label and Mount Devices** window, click **Next**.
12. In the **Review Configuration Settings** window, click **Configure**.
13. Click **Finish**.

## Configuring an autochanger or silo

You can configure a new library resource.

### Procedure

1. Log in to the Console as a NetWorker Administrator.
2. Click the **Enterprise** button  on the taskbar.

3. Highlight a host in the navigation tree, right-click **NetWorker** and select **Launch Application**. The **NetWorker Administration** window appears.
4. Click the **Configuration** button  on the taskbar.
5. Click the **Devices** button  on the taskbar.
6. From the left pane, select **Storage Nodes**.
7. Right-click the storage node for the device and select **Configure All Libraries**.
8. Fill in the requested information and click **Start Configuration**
9. Click **Finish**.

## Labelling media

You can label tapes from the NetWorker Console.

### Procedure

1. Log in to the Console as a NetWorker Administrator.
2. Click the **Enterprise** button  on the taskbar.
3. Highlight a host in the navigation tree, right-click **NetWorker** and select **Launch Application**. The **NetWorker Administration** window appears.
4. Click the **Configuration** button  on the taskbar.
5. Click the **Devices** button  on the taskbar.
6. In the navigation tree view, expand **Libraries** and highlight a library, or select **Devices**.
7. In the **Device list**, right-click a device and select **Label**.

## Scheduling a backup

You can schedule backups from the NetWorker Console.

### Procedure

1. Log in to the Console as a NetWorker Administrator.
2. Click the **Enterprise** button  on the taskbar.
3. Highlight a host in the navigation tree, right-click **NetWorker** and select **Launch Application**. The **NetWorker Administration** window appears.
4. Click the **Configuration** button  on the taskbar.
5. Define schedules, groups, and clients.

## Viewing failed backups

You can view the details for failed NetWorker backups.

### Procedure

1. Log in to the Console as a NetWorker Administrator.
2. Click the **Enterprise** button  on the taskbar.
3. Highlight a host in the navigation tree, right-click **NetWorker** and select **Launch Application**. The **NetWorker Administration** window appears.
4. Click the **Configuration** button  on the taskbar.
5. Click **Monitoring** .

6. Select **Groups** in the docking panel.

## Performing a manual backup

Perform a manual backup of a file or folder, to test the NetWorker installation. The procedure to perform a manual backup is different on Windows and UNIX.

### Performing a manual backup on Windows

Use the NetWorker User program to perform a manual backup Windows. The NetWorker User program provides a graphical interface to perform manual backups.

#### Procedure

1. On a NetWorker client, start the **NetWorker User** program.
2. In the **Change server** window, select or type the name of the NetWorker server
3. In the **Source** and **Destination** client windows, select the current NetWorker client.
4. Click **Backup**.
5. In the left pane of the **Backup** window, click the appropriate directory folder.
6. Select a file or directory file to back up in one of the following methods:
  - Select the directory or file and click **Mark**. To clear an item, click **Unmark**.
  - Right-click the directory or file.

When you mark a directory or file for backup, a check mark appears next to that item.
7. Click **Start**.

The Backup Status window displays the progress of the backup. When the NetWorker server has successfully finished the backup, this message appears:

```
Backup completion time: 2-15-07 3:27p
```

If the backup fails, then:

- Review the NetWorker daemon.raw log file on both the NetWorker server and client hosts. Use the **nsr\_render\_log** program to review the log file in a readable format. The *EMC NetWorker Command Reference Guide* on the EMC Online Support Site describes how to use the **nsr\_render\_log** program.
- The location of the daemon.raw is different on Windows and UNIX:
- On Windows, the log file appears in the C:\Program Files\EMC NetWorker\nsr\logs directory.
  - On UNIX, the log file appears in the /nsr/logs directory.
- To determine the cause, refer to the Troubleshooting section.
  - Review the operating system log files (Application event log on a Windows client) for more information.

### Performing a manual backup on UNIX

Use the **save** program to perform a manual backup from the system prompt.

For example, to back up /tmp/myfile.txt to a server called jupiter, type:

```
save -s jupiter /tmp/myfile.txt
```

The UNIX man pages describe how to use the save program.

## NetWorker services

The main services and programs for the NetWorker server are the NetWorker storage node, NetWorker client and NetWorker Management NMC server.

This section includes information on the NetWorker services, and how to start and stop the services.

For more information about:

- Main NetWorker services, The *EMC NetWorker Command Reference Guide* or the UNIX man pages provides more information.
- Service port requirements when configuring a firewall. The EMC NetWorker Security Configuration Guide provides more information.

## Services and programs on the NetWorker server

There are many NetWorker server services and programs available to configure the NetWorker software.

The following table describes the NetWorker services and programs.

**Table 6** Services or programs on the NetWorker server

Service or program	Function
nsreexecd	Authenticates and processes the NetWorker server remote execution requests and executes the save and savefs programs on the client.
nsrd	<ul style="list-style-type: none"> <li>• Is the master service that controls other services on the NetWorker server, clients, and storage nodes.</li> <li>• Monitors active save or recover program sessions.</li> <li>• In response to a recover session, nsrd will spawn an agent process,ansrd.</li> </ul>
nsrmmdbd	Provides media database management services to the local nsrd and nsrmmd services and records entries in the media database. This is the media management database service.
nsrjobd	Monitors NetWorker activity during a backup or recovery operation.
nsrindexd	Provides a method for inserting entries into the client file index that is based on information passed by the save program.
nsrmmgd	<ul style="list-style-type: none"> <li>• Manages media library operations.</li> <li>• Provides an RPC-based service that manages all jukebox operations on behalf of the nsrd service.</li> <li>• The nsrd service starts only one instance of nsrmmgd on the NetWorker server as needed.</li> </ul>
nsrlogd	Provides support for the NetWorker audit log service and is configured to run on the NetWorker server by default.

**Table 6** Services or programs on the NetWorker server (continued)

Service or program	Function
nsrcpd	<ul style="list-style-type: none"> <li>Started automatically when there is a request to start up the remote client software installation service (client push).</li> <li>Allows users to distribute and upgrade client software from a centralized software repository across a network.</li> </ul>

## Services and programs on the NetWorker client

The nsrexecd service is available for configuration of the NetWorker client.

The following table describes the nsrexecd service.

**Table 7** Services or programs on the NetWorker client

Service or program	Function
nsrexecd	Authenticates and processes the NetWorker server remote execution requests and executes the save and savefs programs on the client.

## Services and programs on the NetWorker storage node

There are many NetWorker storage node services and programs available to configure media and devices for the NetWorker software.

The following table describes the main services or programs on the NetWorker storage node.

**Table 8** Services or programs on the NetWorker storage node

Service	Function
nsrexecd	Authenticates and processes the NetWorker server remote execution requests and executes the save and savefs programs on the storage node.
nsrmmmd	<ul style="list-style-type: none"> <li>Provides device support, generates mount requests, multiplexes save set data during a multiclient backup, and de-multiplexes recover data. It writes the data sent by save to storage media.</li> <li>Fowards storage information to nsrmmdbd for recording in the NetWorker server media database.</li> </ul>
nsrsnmd	<ul style="list-style-type: none"> <li>Provides an RPC-based service to manage all of the device operations that the nsrmmmd process handles on behalf of the nsrd process on the NetWorker server.</li> <li>Ensures that the necessary device operations are actually performed when needed by nsrd.</li> <li>Is automatically invoked by nsrd as required.</li> </ul>

**Table 8** Services or programs on the NetWorker storage node (continued)

Service	Function
	<ul style="list-style-type: none"> <li>Only one nsrsnmd service is run on each storage node with configured and enabled devices.</li> </ul>
nsrlcpd	<ul style="list-style-type: none"> <li>Provides a uniform library interface to the NetWorker media management daemon, nsrmmgd.</li> <li>Manages the library subsystem media, slot, drive and port resources providing control to move and access the resources within the library subsystems.</li> <li>One nsrlcpd is started for each configured jukebox.</li> </ul>

## Services and programs on the NetWorker Management Console server

There are many NetWorker services and programs available for configuring the NetWorker software from the NetWorker Console.

The following table describes the main services or programs on the NetWorker Management Console (NMC) server.

**Table 9** Services or programs on the NetWorker Management NMC server

Service or program	Function
nsreexecd	Authenticates and processes the NetWorker server remote execution requests and executes the save and savefs programs on the client.
gstd	Known as the Generic Services Toolkit (GST), controls other services provided by the NMC server.
httpd	Starts the NMC console on the client through a web browser.
dbsrv12	A database server that manages information pertaining to console management. For example, Console reports.
gstsnmptrapd	<ul style="list-style-type: none"> <li>Monitors SNMP Traps on a managed Data Domain system.</li> <li>Provides the ability to report SNMP Trap events in the NMC Events task.</li> <li>Started only when SNMP Trap monitoring is configured for the Data Domain system.</li> </ul>

## Stop and start the NMC server

To complete some tasks in the NetWorker software, it is required to stop and start the NetWorker Console service.

### Stopping the NMC server on Windows

#### Procedure

- Log in as a Windows Administrator and right-click **My Computer** and select **Manage**.

2. Expand **Services and Applications** and select **Services**.
3. Right-click **EMC GST Service (gstd)**, then select **Stop**.

## Starting the NMC server on Windows

### Procedure

1. Log in as a Windows Administrator and right-click **My Computer** and select **Manage**.
2. Expand **Services and Applications** and select **Services**.
3. Verify that the NetWorker client is running.  
The NetWorker Remote Exec Service (nsreexecd) should have a status of Started. If the service has not started:
  - a. Right-click **NetWorker Remote Exec Service**.
  - b. Select **Start**.
4. Right-click **EMC GST Service (gstd)**, then select **Start**.

## Stopping the NMC server on UNIX

### Procedure

1. Log in as root.
2. Type one of the following commands:
  - Solaris and Linux: `/etc/init.d/gst stop`
  - AIX: `/etc/rc.gst stop`

## Starting the NMC server on UNIX

### Procedure

1. Log in as root.
2. Verify that the NetWorker client is running.

For example, type the following command: `/usr/bin/ps -ef | grep nsr`

If the client is running, a message similar to this appears:

```
root      240      1      0 ?    0:04 /usr/sbin/nsreexecd -s mysrvr
```

If the client is not running, start it.

3. Start the NMC server by typing one of the following commands:
  - Solaris and Linux: `/etc/init.d/gst start`
  - AIX: `/etc/rc.gst start`

## Stop and start a NetWorker server, client, or storage node

This section describes how to manually stop and start the services for a NetWorker server, client, or storage node. In NetWorker 8.0 and later, new attributes have been introduced to configure a NetWorker server to not accept any new backup or recover sessions in preparation of a NetWorker daemon shutdown or server reboot. EMC NetWorker Security Configuration Guide provides more information around how to prevent the NetWorker server from accepting new backup and recover sessions.

## Stopping a NetWorker host on Windows

### Procedure

1. Log in as a Windows Administrator.
2. Right-click **My Computer** and select **Manage**.
3. Expand **Services and Applications** and select **Services**.
4. Right-click **NetWorker Remote Exec Service (nsreexecd)** and select **Stop**.

## Starting a NetWorker host on Windows

### Procedure

1. Log in as a Windows Administrator.
2. Right-click **My Computer** and select **Manage**.
3. Expand **Services and Applications** and select **Services**.
4. Start the appropriate service.
  - NetWorker server: Right-click the **NetWorker Backup and Recover Server** service (**nsrd**) and select **Start**.
  - NetWorker client or storage node: Right-click the **NetWorker Remote Exec Service (nsreexecd)** and select **Start**.

## Stopping a NetWorker host on UNIX

### Procedure

1. Log in as root.
2. Type the following command:

**nsr\_shutdown**

## Starting a NetWorker host on UNIX

### Procedure

1. Log in as root.
2. Type the appropriate startup command.

The backup commands appropriate for the operating system are listed in the following table.

**Table 10** NetWorker startup commands

Operating system	Startup command
Solaris, Linux	/etc/init.d/networker start
HP-UX	/sbin/init.d/networker start
AIX	/etc/rc.nsr

## Stopping a NetWorker host on Mac OS X

The `launchd` daemon/agent manager controls the NetWorker daemons, and NetWorker configures the daemons to run continuously on the host in the background. EMC does not

recommend that you manually stop and start NetWorker daemons under normal operating conditions.

#### Procedure

1. Log in as a Mac Administrator.
2. Open the Mac OS X Terminal application utility.
3. Stop the service by typing the following command:

```
# launchctl unload /Library/LaunchDaemons/com.emc.NetWorker.plist
```

### Starting a NetWorker host on Mac OS X

The `launchd` daemon/agent manager controls the NetWorker daemons, and NetWorker configures the daemons to run continuously on the host in the background. EMC does not recommend that you manually stop and start NetWorker daemons under normal operating conditions.

#### Procedure

1. Log in as a Mac Administrator.
2. Open the Mac OS X Terminal application utility.
3. Start the client by typing the following command:

```
# launchctl load /Library/LaunchDaemons/com.emc.NetWorker.plist
```



# CHAPTER 2

## Backing Up Data

This chapter contains the following topics:

• <a href="#">Scheduled backups</a> .....	60
• <a href="#">Save sets</a> .....	68
• <a href="#">Manual backups</a> .....	71
• <a href="#">Verifying backup data</a> .....	73
• <a href="#">Synthetic full backups</a> .....	73
• <a href="#">Virtual synthetic full backups (for Data Domain systems)</a> .....	84
• <a href="#">Enabling parallel save streams</a> .....	89
• <a href="#">Probe-based backups</a> .....	90
• <a href="#">Client Direct backups</a> .....	92
• <a href="#">Checkpoint restart backups</a> .....	92
• <a href="#">Deduplication backups</a> .....	102
• <a href="#">Backup data encryption</a> .....	102
• <a href="#">Backup data compression</a> .....	103
• <a href="#">Handling data for NetWorker clients on Windows</a> .....	104
• <a href="#">Console server management data backups</a> .....	104
• <a href="#">Windows mount point back ups</a> .....	106
• <a href="#">Windows Content Index Server or Windows Search Index backups</a> .....	108
• <a href="#">Backing up Windows DHCP and WINS databases</a> .....	109
• <a href="#">Windows backup and recovery notes</a> .....	109
• <a href="#">Customizing the backup command</a> .....	112
• <a href="#">Considerations for backing up raw partitions</a> .....	120
• <a href="#">Backing up access control lists</a> .....	121
• <a href="#">BOOT/BCD Data on Windows backups</a> .....	121
• <a href="#">Support for backing up renamed directories</a> .....	121
• <a href="#">Backing up only client file indexes and the bootstrap</a> .....	122

## Scheduled backups

The NetWorker server backs up client data regularly by using scheduled backups. They are preferred over the manual backups because scheduled backups occur automatically, and data can be recovered more easily. Scheduled backups can be performed at any time.

### Scheduled backup planning

This section uses a scenario for accounting department requirements to highlight tasks to consider when planning a scheduled backup.

Example: Planning scheduled backups for the accounting computers

Company XYZ wants to ensure that all of the computers in the Accounting department are backed up according to the requirements listed in the following table. This table also maps each requirement to specific NetWorker features.

**Table 11** Accounting department backup requirements

Requirement	NetWorker feature	More information
Backups occur at the same time.	Backup Schedule Backup Group	<a href="#">Scheduled backup planning on page 60</a> <a href="#">Creating groups for backup clients on page 63</a>
Accounting backups for the past 3 months are available immediately.	Browse Policy	<a href="#">Setting up policies for quick access and long term storage on page 64</a>
Accounting backups for the past 7 years are available, though not necessarily immediately.	Retention Policy	<a href="#">Setting up policies for quick access and long term storage on page 64</a>
Backups are routed to volumes that can be identified as Accounting backup volumes.	Label Template Pools	<a href="#">Setting up a label template to identify volumes on page 64</a> (if Match Bar Code Labels attribute is not used for the Library resource) <a href="#">Setting up a pool to sort backup data on page 67</a>
To avoid unnecessary backups, do not back up files with a .tmp extension.	Directives	<a href="#">Setting up directives for special processing on page 65</a>
The same files and folders are backed up on each accounting computer.	Client resource	<a href="#">Creating a backup Client resource on page 65</a>
Non-accounting data need only be recoverable for one year.	Browse Policy Retention Policy Client resource	<a href="#">Setting up policies for quick access and long term storage on page 64</a> <a href="#">Creating a backup Client resource on page 65</a>

## Scheduled backup creation

You can create a scheduled backup quickly by using the Client Backup Configuration Wizard or through manual configuration in the NetWorker Console.

### The Client Backup Configuration wizard for scheduled backups

The Client Backup Configuration Wizard provides the ability to:

- Create Client resources for scheduled backups.
- Create Group resources.
- Add new clients to existing backup groups.
- Modify existing client configurations.

The wizard supports NetWorker servers and clients in a stand-alone or cluster environment. The *NetWorker Cluster Integration Guide* provides details about creating a client resource for virtual client backups.

**NOTICE**

The Client Backup Configuration wizard cannot be used to configure a NetWorker NDMP client or clients for NetWare.

---

## Client Backup Configuration Wizard requirements

This section contains requirements or constraints specific to the use of the Client Backup Configuration Wizard.

- The wizard user must:
  - Have NetWorker server and client privileges, or have root (UNIX) or Administrator (Windows) privileges.
  - Have Configure NetWorker privileges on the NetWorker server where the scheduled backup is to be configured.
- The NetWorker server's host must be listed in the servers file on the client machine that is being configured for a scheduled backup.
- Communication between the Console server, NetWorker client host, and NetWorker server must use nsrauth strong authentication.
- The Console server, NetWorker client host, and NetWorker server must be using NetWorker 7.5 or later.
- Multiple wizard hosts cannot access the same client machine simultaneously.

## Accessing the Client Backup Configuration Wizard

The wizard opens. If the wizard fails to open, ensure that all prerequisites in are met. Also check the NetWorker daemon log for additional details.

### Procedure

1. From the **Administration** window, click **Configuration**.
2. In the **Configuration** window, click **Clients**.
3. Add a client or modify an existing client:
  - To add a new client, select **Configuration** menu > **Client Backup Configuration** > **New**.
  - To modify an existing client, select the client and then select **Configuration** menu > **Client Backup Configuration** > **Modify**.

## Manual scheduled backup creation in the Console

To exercise more control over scheduled backups than is possible by using the Client Backup Configuration wizard, create the schedule by using the NetWorkerConsole.

You do not have permissions to make configuration selections if the following error message appears while completing any task in this section:

```
user user_name needs to be on administrator's list
```

**NOTICE**

[OS-X Support on page 733](#) provides information about backing up NetWorker clients on Mac OS X.

---

## Creating a schedule for backups

A schedule can be applied to each client backup. Use the following procedure to create a schedule for backups.

### Procedure

1. From the **Administration** window, click **Configuration**.
2. In the expanded left pane, select **Schedules**.
3. From the **File** menu, select **New**.
4. In the **Name** attribute, type a name for the schedule.
5. From the **Period** attribute, select **Week or Month**.
  - Select **Week** to create a weekly backup schedule. For example, if a full backup for a Friday is selected, every Friday will have a full backup.
  - Select **Month** to create a monthly schedule. For example, selecting a full backup for the first of the month will create a full backup on the first of every month.
6. Select a backup level for each day in the weekly or monthly period:
  - a. Select a day.
  - b. Right-click and from the **Set Level** menu, select a backup level.
7. If required, select an override backup level for any day. An override occurs once only for the selected day:
  - a. Select a day.
  - b. Right-click and from the **Override Level** menu, select a backup level.
8. Click **OK**.

## Creating groups for backup clients

A backup group specifies the time of day when a backup occurs.

Creating groups for backup clients enables you to:

- Balance backup loads to reduce the impact on your network and the NetWorker server.
- Sort data to specific backup volumes. To sort data, groups are used in conjunction with backup pools.

To create groups for backup clients:

### Procedure

1. From the **Administration** window, click **Configuration**.
2. In the expanded left pane, select **Groups**.
3. From the **File** menu, select **New**.
4. In the **Name** attribute, type a name for the group.
5. In the **Comment** attribute, type a description of the group.
6. For the **Start Time** attribute, type a new time, unless it is appropriate to maintain the default time of 3:33 A.M. Ensure that start times for different groups are far enough apart so that one group has completed backing up before the next group starts.
7. For the **Autostart** attribute, select **Enabled**.
8. In the **Printer** attribute, type the name of the printer on which bootstrap save set information will be printed.

9. Click the **Advanced** tab.
10. For the **Client Retries** attribute, change the number of retries, if necessary. This value specifies the number of times the NetWorker software attempts to back up a failed client.
11. Click **OK**.

## Setting up policies for quick access and long term storage

Backup clients specify two policies: a browse policy and a retention policy.

- A browse policy determines how long backup data will be available for quick recovery.
- A retention policy determines how long backup data will be available for recovery, though not necessarily quickly. For example:
  - If it is likely that accounting data would need to be recovered within the past year, a browse policy of one year would be appropriate.
  - If the same accounting data had to be recoverable for up to seven years even though the likelihood of needing to recover it was low, a retention policy of seven years would be appropriate.

### Procedure

1. From the **Administration** window, click **Configuration**.
2. In the expanded left pane, select **Policies**.
3. From the **File** menu, select **New**.
4. In the **Name** attribute, type a name for the policy. Choose a name that reflects the length of time for which the policy specifies. For example, if the policy is for 15 months, type 15 months.
5. In the **Comment** attribute, type a comment about the policy.
6. In the **Number of Periods** attribute, type the number of periods applied to the policy. For example, if you choose months for the **Period** attribute and 3 for the **Number of Periods** attribute, then the policy lasts for 3 months (one quarter).
7. From the **Period** list, select a **period**. This attribute works in conjunction with the **Number of Periods** attribute. For example, a quarterly policy is configured in terms of the number of months (3). A week as seven days beginning on Sunday, a month is the calendar month, and a year is the calendar year.
8. Click **OK**.

## Setting up a label template to identify volumes

If you are not using tapes with barcode labels, and the Match Bar Code Labels attribute is not enabled for the Library resource, then every backup volume requires a unique label for identification. The NetWorker server creates a unique label for each volume by applying a label template.

### Procedure

1. From the **Administration** window, click **Media**.
2. In the expanded left pane, select **Label Templates**.
3. From the **File** menu, select **New**.
4. In the **Name** attribute, type a name for the label template.
5. In the **Comment** attribute, type a description for the label template.

6. In the **Fields** attribute, type the label's components. Place each label component on a separate line. The template can use any or all of these components, although at least one range component must be added:
  - Range of numbers — for example, 001-999
  - Range of lowercase letters — for example, aa-zz
  - Range of uppercase letters — for example, AA-ZZ
  - Character string — for example, Accounting

Ranges of numbers or letters change incrementally with each new label. For example:

  - First label: Accounting.001
  - Second label: Accounting.002
  - Third label: Accounting.003
7. Select a **Separator** and click **OK**. If no symbol is selected, the components will have no separators (for example, Accounting001).
8. Click **OK**.

## Setting up directives for special processing

Directives are optional instructions that control how files and directories are processed during backup and recovery. For instance, one could use a directive to skip all temporary files (\*.tmp) during backup.

Other common uses for directives include adding password-protection and data compression to scheduled backups.

### **NOTICE**

Some operating systems contain files and directories that should not be backed up. Use directives to ensure that these files and directories are not backed up. [Preconfigured global directive resources on page 274](#) provides more information.

### Procedure

1. From the **Administration** window, click **Configuration**.
2. In the expanded left pane, select **Directives**.
3. From the **File** menu, select **New**.
4. In the **Name** attribute, type a name for the directive.
5. In the **Comment** attribute, type a description for the directive.
6. In the **Directive** attribute, type the directive instructions. For example, to skip all files on C:\ that have a .tmp extension, type:

```
<< "C:\"
skip: *.tmp
```

7. Click **OK**.

## Creating a backup Client resource

A client is both a physical computer with NetWorker client software installed on it and a NetWorker *resource* that specifies a set of files and directories to be included in a

scheduled backup. A Client resource also specifies information about the backup, such as the backup schedule, the backup group, browse policies, and retention policies.

A single NetWorker client computer can have several Client resources, although clients with the same save set cannot be in the same group. For instance, suppose the accounting data on a computer should be backed up according to a different schedule than the operating system files on the same computer. To accomplish this, one could create two Client resources on each computer: one for accounting data and another for operating system data.

Another common reason to create multiple Client resources for the same computer is to back up large client file systems more efficiently. For instance, one could create two Client resources: one for each file system on a computer. Each Client resource could be scheduled to back up separately.

### Procedure

1. From the **Administration** window, click **Protection**.
2. In the expanded left pane, select **Clients**.
3. From the **File** menu, select **New**.
4. In the **Name** attribute, type the hostname of the NetWorker client computer.
5. In the **Comment** attribute, type a description of the client. If multiple Client resources are being set up for the same host, type a comment that distinguishes the Client resources.
6. From the **Browse Policy** attribute, select a browse policy from the list. The browse policy determines how long backed-up data is available for quick access.
7. From the **Retention Policy** attribute, select a retention policy from the list. The retention policy determines how long backed-up data is available though not necessarily quickly.
8. Select the **Scheduled Backups** attribute.
9. The **Client Direct** attribute, which is selected by default, enables the client to send backup data directly to the storage device, bypassing the storage node.
10. Select the **Block based backup** attribute to perform backups at the block level.
11. From the **Directive** attribute, select a directive from the list, if applicable.
12. In the **Save Set** attribute, type the name of the files or directories to be backed up. Place multiple entries on separate lines. For example, to back up a log file directory named C:\log and all of the data under the directory named D:\accounting, the entries would look similar to:

```
C:\log  
D:\accounting
```

- To back up mapped drives on Microsoft Windows systems, see special instructions at [Backing up mapped drives on Windows systems on page 67](#).
- To back up all client data, type ALL. For Microsoft Windows operating systems, the ALL save set includes the DISASTER\_RECOVERY:\ save set, which includes the WINDOWS ROLES AND FEATURES save set.

#### NOTICE

Some operating systems contain files and directories that should not be backed up. Use directives to ensure that these files and directories are not backed up. [Preconfigured global directive resources on page 274](#) provides information.

- 13.From the **Group** attribute, select a group from the list.
- 14.From the **Schedule** attribute, select a schedule from the list.
- 15.Select the **Backup renamed directories** attribute to back up the files and subdirectories of a renamed directory even if only the name of the directory has changed.  
If this attribute is selected, and a directory is renamed, all files and subdirectories under that directory will be backed up during the next scheduled full or non-full backup.
- 16.On **Globals (2 of 2)**, in the **Owner notification** attribute, specify the command to send a backup completion email to email recipients.
- 17.Click **OK**. The client is now set up for scheduled backups.

### Results

To determine whether a client is enabled for scheduled backups, locate the client entry in the right pane and look for a check mark under the Scheduled backup column.

## Backing up mapped drives on Windows systems

To back up a mapped drive on a Microsoft Windows client for either a scheduled or a manual backup, do not specify the drive letter. Specify the Client resource as follows.

1. Open the **Client Properties** for the client to be backed up.

---

#### Note

Do not combine backups of mapped drives with local backups within the same Client resource instance. An error results. Create a separate instance of the Client resource for all mapped drives that you will access by the same user name and password.

2. On the **General** tab, in the **Save Set** attribute, specify the Universal Naming Convention (UNC) path of the save set to back up.

For example, to specify the accounts directory on the server *jupiter*, type:

```
\\"jupiter\accounts
```

3. On the **Apps & Modules** tab, configure the following:

- Type the **Remote User** and **Password** required to access the UNC path.
- In the **Backup Command** field, type:

```
save -xL
```

- In the **Save Operations** field, type:

```
VSS:*=off
```

## Setting up a pool to sort backup data

A backup pool is a collection of volumes to which backup data is written. Use pools to sort backup volumes so that the volumes are easy to locate when they are needed.

### Procedure

1. From the **Administration** window, click **Media**.
2. In the expanded left pane, select **Media Pools**.
3. From the **File** menu, select **New**.

4. In the **Name** attribute, type a name for the pool. A pool is associated with a label template. Use a name that clearly associates the pool with the corresponding label template.
5. In the **Comment** attribute, type a description of the pool.
6. Select the **Enabled** attribute.
7. For the **Pool Type** attribute, select **Backup**.
8. In the **Label Template** attribute, select the matching label template.
9. Modify the attribute to use to direct specific backup data to the volumes belonging to this pool. Data can be sorted by group, backup clients, save sets, and backup levels.
10. Click **OK**.

## Creating Schedules

### Procedure

1. From the **Administration** window, click **Configuration**.
2. In the expanded left pane, select **Schedules**.
3. From the **File** menu, select **New**.
4. In the **Name** attribute, type a name for the schedule.
5. From the **Period** attribute, select **Week or Month**.
  - Select **Week** to create a weekly backup schedule. For example, if a full backup for a Friday is selected, every Friday will have a full backup.
  - Select **Month** to create a monthly schedule. For example, if a full backup for the first of the month is selected, every month will have a full backup on the first of the month.
6. Select a backup level for each day in the weekly or monthly period:
  - a. Select a **day**.
  - b. Right-click and from the **Set Level** menu, select a backup level.
7. If required, select an override backup level for any day. An override occurs once only for the selected day:
  - a. Select a **day**.
  - b. Right-click and from the **Override Level** menu, select a backup level.
8. Click **OK**.

## Save sets

A Client resource identifies the client data to be backed up. The collection of data items backed up during a backup session between the NetWorker server and the Client resource is called a *save set*. A save set can consist of the following:

- A group of files or entire file systems.
- Application data, such as a database or operating system settings.

**NOTICE**

---

A save set is defined when a Client resource is created.

## Predefined save sets for scheduled backups

In addition to entering files or file systems in the Save Set attribute of the Client resource, you can also type the names of predefined save sets when configuring the NetWorker client.

For Windows, the predefined save set DISASTER\_RECOVERY:\ is available.

Consider the following:

- The DISASTER\_RECOVERY:\ save set backs up critical volumes, UEFI, the system reserved partition, and WINDOWS ROLES AND FEATURES. The DISASTER\_RECOVERY:\ save set does not include data for clusters, Active Directory, DFS-R, and Windows Server Failover Cluster.
- Checkpoint restart backup for the Windows DISASTER\_RECOVERY:\ save set is not supported. If a Client with a DISASTER\_RECOVERY:\ save set is checkpoint-enabled, it is quietly ignored for the Disaster Recovery save sets. The save set will be marked with a cb flag instead of a k flag, indicating that the checkpoint is not considered for Disaster Recovery.
- The save set ALL includes all predefined save sets, including the DISASTER\_RECOVERY:\ save set. See the preceding bullet regarding checkpoint-enabled backups and the DISASTER\_RECOVERY:\ save set.

## The ALL save set

The ALL save set is the default save set used when a client is created.

The following table provides a list of the save sets that are included in the ALL save set.

**Table 12** Components in the ALL save set

Operating system	Files
UNIX	<ul style="list-style-type: none"> <li>• When the backup starts, the savefs process will read the contents of the /etc/vfstab file on Solaris clients, the /etc/fstab file on HP-UX and Linux clients, or the /etc/filesystems file on AIX clients. The contents of the file are compared to the currently mounted file systems. Only currently mounted file systems that are configured in the files mentioned above are backed up.</li> <li>• For a Solaris sparse or whole root zone client, all mounted file systems in the sparse or whole root zone that are not normally skipped, such as NFS, are backed up.</li> <li>• ZFS filesystems are backed up.</li> <li>• If the save set name includes a symbolic link, a save set recovery is not supported.</li> </ul>
Windows	<ul style="list-style-type: none"> <li>• DISASTER_RECOVERY:\</li> <li>• Non-critical volumes The section <a href="#">Overview of Windows Bare Metal Recovery (BMR) on page 613</a> provides more information about the data contained in the DISASTER RECOVERY save set.</li> </ul>
Mac OS X	All local and mounted volumes

## File system objects not included in the ALL save set

The ALL save set excludes certain named directories, file systems, and files. A list of the file system object names that the ALL save set does not back up includes:

• hsfs	• nfs4	• usbfs
• proc	• nfs	• devpts
• fd	• brfs	• smbfs
• cachefs	• msdos	• cifs
• lofs	• dfs	• swap
• mntfs	• autofs	• tmp
• ctfs	• iso9060	• tmpfs
• objfs	• udf	• nucfs
• sharefs	• sysfs	• nucam
• nfs2	• debugfs	• fdfs
• nfs3	• subfs	• xx
• nfs3perf	• usbdevfs	• none
• profs	• binfmt_misc	

## Save set ALL keywords for scheduled file system backups

You can use special keywords with the save set ALL to define the file systems to include in a client backup. The following table provides a list of the special ALL save sets and the backup behavior.

### NOTICE

When the All save set is used for a back up, the Networker software creates a temporary file similar to a directive under each drive. The file is named by using the format, <drive guid>.txt. The file lists the files that are excluded from the backup. The file is temporary and is automatically deleted when the backup completes.

**Table 13** Special ALL save sets

Special ALL save set syntax	Backup behavior
all- <i>filesystem</i>	<ul style="list-style-type: none"> <li>Only backup locally mounted file systems of a particular type. For example, the all-zfs save set backs up all locally mounted zfs file systems on a Solaris host.</li> <li>Other save sets include: all-ntfs and all-ext3.</li> <li>File systems that are normally skipped such as NFS are still skipped.</li> <li>The <i>NetWorker Software Compatibility Guide</i> provides a list of the supported file system for each operating system.</li> </ul>
all-mounts	<ul style="list-style-type: none"> <li>On UNIX clients, backup all of the currently mounted file systems. File systems that are normally skipped such as NFS are still skipped.</li> </ul>

**Table 13** Special ALL save sets (continued)

Special ALL save set syntax	Backup behavior
	<ul style="list-style-type: none"> <li>On Windows clients, the all-mounts save set is equivalent to the save set ALL.</li> </ul>
all-local	<ul style="list-style-type: none"> <li>For a global zone client, the file systems in the sparse or whole root zone on the physical host are backed up. File systems in the global zone are skipped.</li> <li>For a Sparse or Whole Root zone client, the save set is equivalent to the save set ALL.</li> </ul>
all-global	<ul style="list-style-type: none"> <li>For a global zone client, all file systems in the global zone are backed up. All sparse and whole root zone file systems on the physical host are skipped.</li> <li>For a Solaris sparse or whole root zone client, the save set is equivalent to the save set ALL.</li> </ul>

## Manual backups

Manual backups enable users to make quick backups of a few files. Unlike scheduled backups, manual backups do not:

- Generate bootstrap files
- Back up indexes

This may present recovery problems if the indexes are recovered after a disaster, but before a scheduled backup has backed up the latest indexes. For this reason, scheduled backups are the preferred backup method. However, indexes can be saved manually by using the `savegrp` program.

On Microsoft Windows, manual backups can be performed by using the graphical NetWorker User program. On UNIX and Linux, manual backups can be performed from only the command line.

### NOTICE

You can also start a scheduled backup manually.

## Performing a manual backup on Windows

The NetWorker User program cannot be used to back up deduplication data. Deduplication data must be backed up by using scheduled backups or from the command line.

### Procedure

- In the **NetWorker User** program, click **Backup**.
- In the left pane of the **Backup** window, click the appropriate directory folder. To provide you with the ability to perform an offline restore (Windows BMR), select the **DISASTER\_RECOVERY** save set.
- Select each directory or file, and click **Mark**. To clear an item, click **Unmark**.
- Click **Start** to begin the manual backup. The **Backup Status** dialog box displays the progress of the backup.

When the backup finishes, a message similar to this appears:

Backup completion time: 2-15-07 3:27p

If the backup fails due to a problem with VSS or a writer, an error message appears. Use the Windows Event Viewer to examine the event logs for more information. VSS backup error messages are also written to the NetWorker log file.

**NOTICE**

Certain kinds of corrupt files or errors on computer disk volumes are not detected. NetWorker might back up this corrupt data. To avoid this situation, run diagnostic programs regularly to correct disk volume errors.

## Excluding file type devices from a manual backup on Windows

When performing a NetWorker User backup on a NetWorker server or storage node that is backing up to a local file type device, do not include the local file type device in the backup. If the local file type devices are included, the backup file will grow until there is no more disk space. The following procedure must be performed before selecting any files for backup or archiving, or before performing any activities from the Operation menu of the NetWorker User program.

You can ensure that file type devices are excluded from NetWorker User backups by creating a local directive on the NetWorker server.

### Procedure

1. Start the **NetWorker > User** program.
2. From the **Options** menu, select **Local Backup Directives**.
3. Click the filename of any file device to unmark it.
4. From the **File** menu, select **Save Directive**. This creates a directive file named `networkr.cfg`.
  - [Local directives within the NetWorker User program on page 273](#) provides more information about the `networkr.cfg` file.
  - [File type devices on page 156](#) provides information about file type devices.

## Performing a manual backup from the command prompt

A manual backup can also be performed from the command prompt by using the `save` command.

For example, to back up `myfile` to the server *jupiter*, type:

```
save -s jupiter myfile
```

If you do not specify the `-s` option with the `save` command, the file(s) will be backed up to the NetWorker server defined in the `/nsr/res/servers` file that comes first in alphabetical order.

**NOTICE**

You can also manually back up the bootstrap and indexes for a group by using the `savegrp` program with the `-O` option and a group name. The *EMC NetWorker Command Reference Guide* or the UNIX man pages provides information about `save` and `savegrp`.

# Verifying backup data

## NOTICE

This feature is not available on UNIX clients.

---

Use the NetWorker Verify feature to ensure that backup data on the NetWorker server matches the data on the local disk. The Verify feature compares the file types, file modification times, file sizes, and file contents. It does *not* verify other system attributes, such as read-only, archive, hidden, system, compressed, and file access control list (ACL). The NetWorker server alerts you to any changes that have occurred to your data since the backup. Verification also determines whether a hardware failure kept the NetWorker server from completing a successful backup. The Verify feature provides a way to test the ability to recover data.

## NOTICE

To verify files, you must have Windows Administrator privileges for the computer.

---

### Procedure

1. In the **NetWorker User** program, select **Verify Files** from the **Operation** menu.
2. Select the data items to be verified.
3. Click **Start**.

### Results

You can monitor the data verification progress in the Verify Files Status window. After the verification is complete, the Verify Status dialog box shows any data discrepancies.

# Synthetic full backups

A synthetic full backup combines a full backup and subsequent incremental backups to form a new full backup which is called a synthetic full backup. A synthetic full is equivalent to a traditional full backup and can be used in all of the same ways as a traditional full backup. Although the synthetic full backup method is quite different from the traditional method of creating a full backup, the result is exactly the same.

The synthetic full save set includes data that was backed up between the full backup and the last incremental backup. After a synthetic full backup is performed, the next synthetic full backup combines the previous synthetic full backup and subsequent incremental backups.

The full backups and incremental backups must be created with NetWorker 8.0 and later. Synthetic full backups cannot be created using full, level, or incremental backups that were created with NetWorker versions prior to NetWorker 8.0. This feature supports filesystem backup only.

Using synthetic full backups reduces recovery time because the data is restored from the single synthetic full backup instead of from the last full backup and the incremental backups that follow it. The save sets that result from a synthetic full backup are equivalent to a traditional full backup of these same clients as of the time of the last incremental backup that was used in the creation of the synthetic full backup. Each synthetic full backup forms the basis upon which the next synthetic full is created.

Synthetic full backup is supported on Avamar deduplication nodes by using the nsrconsolidate command. The synthetic full backup rehydrates (reverts) the deduplicated data to its original non-deduplicated state.

**NOTICE**

NetWorker 8.0 and later does not support the consolidate backup level. During an upgrade from a previous release of the NetWorker server software to version 8.0 or later, the update process changes the value in the Level attribute from Consolidate to NULL.

NetWorker 8.1 SP1 and later does not support the synth\_full backup level in the Level attribute of a Group resource. During an upgrade from a previous release of the NetWorker server software to version 8.1 SP1 or later, the update process changes the value in the Level attribute from synth\_full to NULL. To perform a synthetic full backup, in the Level attribute of the Group resource, select incr\_synth\_full. The synth\_full backup level is not displayed in the Level dropdown list in the Group resource.

---

Synthetic full backups do not eliminate the requirement for full backups. It is best practice to schedule and perform full backups on a monthly or quarterly basis and limit the number of incremental backups.

## Differences between a synthetic full backup and a traditional backup

When traditional full backups are performed, data from the clients is sent over the network to the storage nodes. In some cases, this can have a negative effect on client network performance.

In contrast, to create a synthetic full, the NetWorker software:

- Analyzes an existing full backup along with subsequent incremental backups.
- Extracts from each of these the most current versions of files in the backup set.
- Streams them into a new full backup.

Synthesizing the new full backup does not involve the client machines and localizes the network traffic to the NetWorker server and storage nodes.

**NOTICE**

When you use the ALL save set with synthetic full and virtual synthetic full backups, the non-critical volumes save successfully. However, critical volumes including DISASTER\_RECOVERY:\ are not backed up. The nsrconsolidate() command is unable to process the DISASTER\_RECOVERY:\ saveset. The client then runs a level full backup for the DISASTER\_RECOVERY:\ saveset.

## When to use synthetic full backups

Synthetic full backups can be used on any eligible client. However, synthetic full backups, provide the most benefit in the following cases:

- If the backup window is less than the amount of time it takes to perform a full backup.
- A client is at a remote location and data transfer over the network to the server is a performance issue for either the network or the client.
- Network bandwidth is small.
- Large backups over the network are cost-prohibitive.

Synthetic full backups involve only the NetWorker server and storage node. If all of the data is located on a few storage nodes, then the network overhead for creating the synthetic full can be drastically reduced when compared to a traditional full backup of the same save sets.

**NOTICE**

Under most conditions, synthetic full backups can free network bandwidth and Client resources. However, a synthetic full backup might take longer to run than a full backup because incremental backups are combined into a synthetic full backups. Used indiscriminately, synthetic full backups might impact the performance of the storage node.

Synthetic full backups do not eliminate the requirement for full backups. It is best practice to schedule and perform full backups on a monthly or quarterly basis and limit the number of incremental backups.

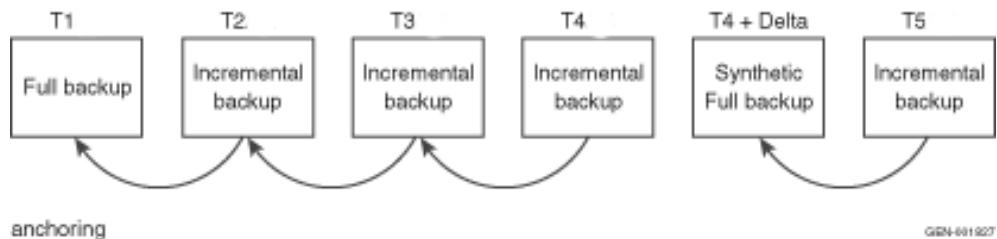
## How a synthetic full backup is created

Synthetic full backups are based on the last successful incremental backup in the chain of incremental backups.

The following figure illustrates how a synthetic full backup is created.

**Figure 6** Synthetic full backups

### Save time



GEM-IN1827

In this example, a synthetic full backup is created by combining the full backup at T1 with the subsequent incremental backups at T2, T3, and T4 to form a new full backup which is called a synthetic full backup at T4 + Delta. The save set at T4 + Delta is equivalent to a full backup that is taken at T4.

The T4 + Delta represents a small time change of one or two seconds from the time of T4, since two separate save sets can not be assigned the exact same save set time. For example, if T4 is created at 1334389404, then T4+Delta is created at 1334389405, a difference of one second. The synthetic full save set will only include files covered by save sets up to T4 at 1334389404. The incremental backup following the synthetic full backup at 1334389405 will include all changes since 1334389404. Note that the synthetic full backup does not include the changes since T4, since only one save set can exist at any given time.

The synthetic full save set includes data that was backed up between the full backup and the last incremental backup of the client from a point-in-time after the last successful incremental backup in the chain that was recorded in the media database. After a synthetic full backup is performed, the next synthetic full backup combines the previous synthetic full backup and subsequent incremental backups.

Given that the synthetic full backup is based upon the last successful incremental backup in the chain of incremental backups, if T3 and T4 are removed from the chain of incremental backups, then the synthetic full backup is taken at T2 rather than T4.

## Synthetic full requirements

There are several requirements to consider before performing a synthetic full backup.

Ensure that the following requirements are met:

- A full or synthetic full backup was created with NetWorker 8.0 or later before subsequent synthetic full backups are run. If a full backup does not exist, the synthetic full backup will fail with the following error:

```
Synthetic full operation must include one full save
```

To resolve this issue, perform a full backup and incremental backups of the save sets which will be participating in synthetic full backup.

- All incremental backups participating in the synthetic full backup are in the media database. If one of the incremental backups are missing, the synthetic full backup might fail with the following errors:

```
nsrconsolidate: info, Anchor saveset time time (machine_name:path)
not found in media database.
savegrp: Check criteria for machine name:path returned: Anchor
saveset time time (machine_name:path) not found in media database.
```

To resolve this issue, perform an incremental synthetic full level backup. This backup level creates an incremental backup of the client from a point-in-time after the last successful incremental backup in the chain of incremental backups that was recorded in the media database. A synthetic full backup is then automatically run.

- All save sets participating in the construction of a synthetic full save set must:
  - Retain the same client name during the incremental and full backups that combine to form the synthetic full backup.
  - Retain the same save set name during the incremental and full backups that combine to form the synthetic full backup.
  - Be browsable in the online index. If one of the save sets to be used in the synthetic full backup is no longer browsable, the synthetic full backup will fail with the following error:

```
Save set saveset invalid for consolidate: no longer browsable.
```

- Have the backup renamed directories attribute enabled (default setting) for all clients that participate in the synthetic full backup. [Enabling backup renamed directories on page 77](#) provides instructions on setting this attribute if the backup fails with an error message.
  - Have a client resource created for the NetWorker storage node that will be used for the synthetic full backup. A client connection license for this storage node is not used if the storage node is not backed up.
  - Have two available attached devices; one for reading and one for writing. Devices that support concurrent read/write access can be shared for reading and writing, if the pool restrictions and session limits allow for the use of the device.
- Consider the following:
- Use Advanced File Devices and DataDomain devices to store all of your backups to a single device.
  - A synthetic full backup can not be saved to a file device or tape volume that contains backups which will be used to create the synthetic full backups.

- Use the following criteria to determine the recovery storage node:
  - If the required volume is not mounted, the recovery storage node is selected based on the setting in the client's recovery storage node attribute.
- If the required volume is already mounted, the storage node where the volume is mounted will be selected for recovering the data.

## Enabling backup renamed directories

If the backup renamed directories attribute is not enabled during any of the full or incremental backups that participate in the synthetic full backup.

The synthetic full backup might fail with the following error message:

```
Save set saveset invalid for consolidate: backup renamed directory
index lookup information missing from index
```

### Procedure

1. Enable **backup renamed directories** for all clients that are participating in the synthetic full backup. The Backup renamed directories attribute is found in the Client resource.
2. Perform a full backup.
3. Perform at least one incremental backup.
4. Perform a synthetic full backup.

## Limitations of synthetic full backups

The synthetic full operation is resource intensive. In order to manage resource usage, it is best practice to perform synthetic full operations outside of the normal backup window.

Do not perform a synthetic full backup, if:

- The backup type is NDMP, SCSI, or VCB.
- The save set belongs to a snapshot group.
- The save sets contain backups of raw disk file partitions.
- The save sets contain database systems such as Microsoft Exchange and Oracle.
- The backup command with save is not used.
- The save set attribute contains the DISASTER RECOVERY:\ save set or the ALL save set on Windows. [Synthetic full backups on page 618](#) describe how the synthetic full backup feature works with Windows offline disaster recovery.

For UNIX clients, include the forward slash to designate root "/" when specifying a save set name. Otherwise, the synthetic full backup will fail. For example, if /tmp is misspelled as tmp in the save set list of the Client resource, the backup will fail.

For Windows clients, include the backslash "\\" when specifying a drive letter in a save set name. Otherwise, the synthetic full backup will fail. For example, if D: is typed in the save set list of the Client resource, instead of D:\\, the synthetic full backup will fail.

**NOTICE**

Synthetic full backups can free network bandwidth and Client resources by reducing the backup window. However, because incremental backups are combined into a synthetic full, a synthetic full backup might take longer to run on the storage node than a comparable full backup. Without proper planning, synthetic full backups might impact the performance of the storage node.

A synthetic full operation is resource intensive. In order to manage resource usage, it is best practice to perform synthetic full operations outside of the normal backup window.

## Recommended devices for synthetic full backups

Although synthetic full backups can be directed to any device that can be used in a traditional full backup, there are special considerations to account for when conducting synthetic full backups. Since synthetic full backups involve concurrent recover and save operations, it is strongly recommended that the synthetic full be directed to devices which can perform concurrent operations such as Data Domain devices or Advanced File Type Devices (AFTDs). Using these device types allows the NetWorker software to automatically handle volume contention, where the same volume is required for both reading and for writing simultaneously. These devices typically offer better performance.

Other devices such as tape drives, VTLs, and basic file devices can be used as the destination for synthetic full backups but careful preparation is required if the backup is to succeed. The backup must be configured so that the destination volume does not contain any of the source save sets that are used for the synthetic full backup. Also, for tape media, ensure that there is enough available drives to allow for concurrent recovery of the source data and for saving the synthetic full backup. Without careful planning, synthetic full backups to tape, VTL or basic file devices might stall because of volume contention.

## Synthetic full scheduling considerations

A synthetic full operation is resource intensive because it concurrently performs both recover and save operations. As a result, perform synthetic full operations outside of the regular backup window. You can do this by creating separate groups for synthetic full operations. When using synthetic full backups, do not exceed the time interval of one month between traditional full backups.

To maintain current resource usage which is defined as the space usage in the backup media and client file indexes, run synthetic full backups in place of traditional full backups. Running synthetic full backups more frequently than traditional backups are currently run results in the consumption of more space in the backup media and client file indexes.

For example, if the current backup schedule performs a full backup once a week, the full backup can be replaced with an incremental backup followed by a synthetic full backup without increasing the backup space usage.

A suggested change for using synthetic full backup for the following schedule is:

```
Current schedule: Sunday : Full, Mon-Sat : Incr
New Schedule: First Sunday : Full, Mon-Sat : Incr, 2nd - 5th Sun :
incr followed by synth_full.
```

## Synthetic full and backup levels

NetWorker 8.0, NetWorker 8.0 SP1, and NetWorker 8.1 and later support two synthetic full backup levels.

The NetWorker backup levels are:

- synth\_full, defined in a Schedule resource.
- incr\_synth\_full, defined in Level attribute of a Group or the Schedule resource.

Prior to NetWorker 8.0, performing a backup at a particular level created a backup of that same level. However, synthetic full backups do not follow this convention. Performing a synthetic full backup creates a full level backup. The [Schedules on page 256](#) and [Backup levels on page 263](#) sections provide more information.

In NetWorker 8.1 SP1 and later, synth\_full is no longer an available attribute in the Group Properties dialog. If you want to create a synth\_full backup you can create one outside of the Group backup window by configuring a backup with a different schedule.

The following table shows the level backups that are created by synthetic full and incremental synthetic full backups.

**Table 14** Synthetic full backup levels

Backup level	Reported backup level
synth_full	full
incr_synth_full	incr full

### Incremental Synthetic Full

Synthetic full backups only cover the period in time up to the last incremental backup that was used in the synthesizing process. To backup data that has changed since that last incremental backup, you must perform an incremental synthetic full backup. During an incremental synthetic full backup, the NetWorker software performs an incremental backup of the save set and then adds that to the full and incremental backups that are already in place for the synthetic full process and then performs the synthetic full backup.

## Synthetic full backups

You can schedule synthetic full backups from the Administration window, or perform a manual incremental synthetic full backup from the command prompt.

### Configuring synthetic full backups from the Administration window

You can configure a scheduled synthetic full backups.

#### Procedure

1. Ensure the NetWorker server, storage node, and clients are at NetWorker 8.0 or later.
2. For each storage node that participates the synthetic full backup, ensure that a client resource has been created for that storage node.
3. For each NetWorker client that participates in the synthetic full backup:

- a. Ensure that the **Backup renamed directories** attribute is enabled.

New client instances created with NetWorker 8.0 have the Backup renamed directories attribute enabled by default.

- b. In the **Save Set** attribute, type the name of the files or directories to be backed up:

- For the Microsoft Windows operating systems, even though most file systems are case-independent, you must use the same path name case that the Windows file system uses. The NetWorker software's cross-platform indexing system is case-sensitive. It is best practice to always specify the Windows drive letter in upper case.
- Place multiple entries on separate lines. For example, to back up a log file directory named C:\Docs\CustomerLogs and all of the data under the directory named D:\accounting, the entries would look similar to:

```
C:\Docs\CustomerLogs
D:\accounting
```

- On Windows, when specifying a drive name, always use the backslash “\” otherwise, the synthetic full backup will fail. For example, to specify the D: drive, type D:\.
- On UNIX, include the forward slash to designate root "/" when specifying a save set name. Otherwise, the synthetic full backup will fail. For example, if /tmp is misspelled as tmp in the save set list of the Client resource, the backup will fail.

4. Create a **Group** for the synthetic full backups:

- Ensure that the groups that are used for the synthetic full backup operations contain only the save sets that are compatible with synthetic full backup operations. [Limitations of synthetic full backups on page 77](#) provides details. The save sets that are incompatible with synthetic full feature are reported as failed save sets in the savegrp log file.
- Configure Windows clients within a dedicated group; not mixed with UNIX clients.
- If multiple groups have been configured to run concurrently, set the Parallelism attribute in the client resource that was created for the NetWorker server to 40. You can find the Parallelism attribute in the Globals (1 of 2) tab of the Client property dialog box. This limits the number of concurrent synthetic full operations to 20. The Parallelism setting should be divided by 2 to formulate the number of concurrently running synthetic full operations.

The number of concurrent synthetic full operations in a data zone should be limited to 20.

The optimal number of concurrent synthetic full operations operation depends on the following:

- Configuration of the NetWorker server
- Size of the save sets, number of clients
- Number of savegrp instances that are concurrently running
- Number of other active operations, such as cloning that are concurrently running.

5. Open the schedule to which the synthetic full backup will be applied, and use either of the following:

- Preconfigured Incr+Synthetic Full schedules:

Using one of these schedules forces the NetWorker software to perform an incremental backup prior to performing a synthetic full back. This backs up all of

the data that has changed since last full backup and subsequent incrementals to create a synthetic full backup:

- Incr+Synthetic Full 1st Friday of Month
- Incr+Synthetic Full Every Friday
- Incr+Synthetic Full 1st of Month
- Incr+Synthetic Full Quarterly
- Create a new schedule that uses the Synthetic Full+Incr backup level — Using this schedule will force the NetWorker software to perform an incremental backup of the save group immediately prior to performing a synthetic full.

Use this level when synthetic full backups fail because the incremental backup chain is broken or one or more incremental backups did not have Backup renamed directories attribute enabled. This level triggers an incremental to be created before the synthetic full backup. This mends the broken chain of incremental backups. [Scheduled backup planning on page 60](#) provides information about creating a schedule.

#### **NOTICE**

For Windows clients, ensure that the backup levels in the schedule are equal to or greater than the previous backup level. This prevents renamed files from being skipped when the synthetic full backup is created. For example, if mixed backup levels are run before a synthetic full backup is run, renamed files might not be included in the synthetic full backup since the level backup following the incremental backup might not include the renamed files.

## Performing manual incremental synthetic full backup by using the savegrp program

The savegrp program can be run from the command line of the NetWorker server to perform an incremental synthetic full level backups of a particular group.

The `-l` option is used to indicate that the backup level is a synthetic full or incremental synthetic full. The *EMC NetWorker Command Reference Guide* or the UNIX man pages provide more information.

For example:

```
savegrp -N 20 -l inc_synth_full group_name
```

The `-l incr_synth_full` option initiates an incremental backup from the client system before running the synthetic full process. This ensures the time difference between T4 and T4+delta is minimized.

## Performing manual synthetic full backups using nsrconsolidate

Run the nsrconsolidate program from the command line of the NetWorker server to perform more granular synthetic full backup. It cannot be used to perform an incremental synthetic full level backup of a particular group.

The nsrconsolidate command can be used to define backup data to be included in the synthetic full backup by:

- client name and save set name
- ssid/cloneid
- time range

The nsrconsolidate command can be used to create synthetic full backups of data stored on an Avamar deduplication node. The deduplicated data is rehydrated (reverted) to its original non-deduplicated state.

**NOTICE**

For the Microsoft Windows operating systems, even though most file systems are case-independent, you must use the same path name case that the Windows file system uses when specifying a save set name, client name, file, or directory. The NetWorker software's cross-platform indexing system is case-sensitive. It is best practice to always specify the Windows drive letter in upper case.

When running the nsrconsolidate command, it is best practice to run fewer nsrconsolidate commands that include many save sets than to run multiple nsrconsolidate commands with a fewer number of save sets. This helps nsrconsolidate to manage the number of concurrent synthetic full operations and reduce resource usage.

The optimal number of concurrent nsrconsolidate operations depend on the following:

- NetWorker server configuration
- Size of the save sets
- Number of clients
- Number of savegrp instances that are running concurrently
- Number of other active operations, such as cloning that are running concurrently

The *EMC NetWorker Command Reference Guide* or the UNIX man pages provide more information.

## Checking the integrity of a synthetic full backup

**Note**

If the clones option is enabled for the group, all backups will be cloned including the synthetic full backup.

If a synthetic full backup fails because the incremental backup chain is broken or one or more incremental backups did not have Backup renamed directories attribute enabled, you can change the level attribute in the Group resource to incr\_synth\_full. This level triggers an incremental to be created before the synthetic full backup. This mends the broken chain of incremental backups.

**Procedure**

1. Open the group that contains the clients that are participating in the synthetic full backup.
2. In the **Advanced** tab of the properties of the group:
  - If not already enabled, enable the **Verify synthetic full** option to verify the integrity of the new indexes entries that are created for the synthetic full backup in the client file index.
  - If not already enabled, enable the **Revert to full when synthetic full fails** option to force the group to perform a full backup on the save set if the synthetic full backup fails.

## Changing the backup group level

Running the savegroup mends the broken chain of incremental backups by triggering a new incremental backup to be created prior to the next synthetic full backup.

### Procedure

1. Open the group that contains the clients that are participating in the synthetic full backup.
2. In the **Advanced** tab of the properties of the group, select **incr\_synth\_full** from the **level** attribute.
3. Click **Ok**.

## Checkpoint restart considerations with synthetic full backups

Backups that are performed during a checkpoint restart might be included in a synthetic full backup if the standard Synthetic full requirements are met.

[Synthetic full requirements on page 76](#) provides more information.

[Checkpoint restart backups on page 92](#) provides more information on how to configure and use checkpoint restart backups.

## Synthetic full backup reporting

You can obtain information on synthetic full backups by using NetWorker reporting.

When defining the backup statistics or backup status report in the Console:

- For the Save Sets Details report, the value Synthetic in the Type column indicates that the backup is a synthetic full.
- For the Save Sets Details by client report, the value Synthetic in the Type column indicates that the backup is a synthetic full.

## Running queries on synthetic full backups

You can view information on partial save sets by using queries.

### Procedure

1. In the **Administration** window, click **Media**. Media-related topics appear in the navigation tree.
2. Select **Save Sets**.
3. Select the **Query Save Set** tab.
4. Click **Select From** in the Type pane and then click the **Synthetic Full** checkbox.
5. Select the **Save Set List** tab to view the result of the save set query.
6. Review the Type column. **Synthetic Full** appears in the Type column if the save set is part of a synthetic full backup.

## Monitoring

A new table called Synthetic Full Sessions is available in the Monitoring section of the console. It contains one row for each client and save set pair.

## Directives

The following directives can be used when performing synthetic full backups:

- compressasm
- aes (encryption)

When using directives with synthetic full backups, consider the following:

- If directives were applied to save sets during the full and incremental backups that participate in the synthetic full backup, the synthetic full backup will not remove those directives.
- If any directives including the compressasm or aes directives were applied to the full and incremental backups that participate in the synthetic full backup; these directives will not be applied again.
- If the target volume for the synthetic full backup is a Data Domain device, directives should not be set for the synthetic full backup.
- If an unsupported directive is specified during a synthetic full backup, the directive is ignored.

Review the nsrconsolidate syntax in the *EMC NetWorker Command Reference Guide* or the UNIX man pages for more information.

**NOTICE**

Directives cannot be used with virtual synthetic full backups, so this option must be disabled prior to running the backup. When applying directives to traditional synthetic full backups, ensure that the virtual synthetic full option is unchecked in NMC. [Virtual synthetic full backups \(for Data Domain systems\) on page 84](#) provides more information.

## Directing data from a synthetic full backup to a dedicated pool

You can direct consolidated save sets to a specific set of media.

### Procedure

1. Create a **Group** for consolidation backups.
2. Create a **Pool** for consolidation backups.
3. In the **Pool** resource, select the group that was created for the consolidated backup as the value for the **Groups** attribute.
4. Edit the **Group** attribute in each **Client** resource that is to have consolidated backups, and assign to the group that you created for the consolidated backup.

## Virtual synthetic full backups (for Data Domain systems)

A virtual synthetic full (VSF) backup is the same as a synthetic full backup, except that it is performed on a single Data Domain system. Similar to synthetic full, VSF uses full and partial backups to create a new full backup. However, since the backup occurs on a Data Domain system using new DD Boost APIs, the backup does not require save set data to be sent over the wire, resulting in improved performance over synthetic full and traditional backups.

The following table compares traditional synthetic full and virtual synthetic full.

**Table 15** Traditional synthetic full and virtual synthetic full backups

Traditional synthetic full	Virtual synthetic full
Data is read from and written to volumes	Data movement is limited within the same DDR
Supports read/write for all types of volumes	Only Data Domain devices are supported, and the source and destination volumes must belong to the same DDR. As per the DDBoom API, there are no restrictions if the volumes belong to different M-Trees in the same DDR.
Client file index created by nsrrecopy	Client file index created by nsrconsolidate
Does not require Client Direct support	Requires Client Direct support
Supports Avamar save sets	Cannot use Avamar save sets for creating the virtual synthetic full.

## Virtual synthetic full requirements

There are several requirements that must be met before running virtual synthetic full (VSF) backups.

VSF requires the following:

- DDOS version 5.3 is the minimum supported DDOS version that supports NetWorker VSF backup and clone.
- DDBoom version 2.6; this version of DDBoom is shipped with NetWorker 8.1.
- The DDR must have virtual synthetics enabled.
- All of the constituent backups must be on the same DDR.
- Only non-Avamar clients are supported.

---

### Note

If all the required Avamar deduplicated save sets are rehydrated to the same DDR prior to initiating a VSF, a VSF backup can be performed, but not recommended.

- The client must have the Client Direct attribute enabled. Also, a value is required in the volume location attribute for a Data Domain device. NetWorker updates the volume location attribute during the device mount operation. Before you update a storage node that uses Data Domain devices, unmount each device. Once the update completes, mount each device.
- The DDR must have virtual-synthetics enabled. When you log into the Data Domain system and run ddboost option show, ensure that the output indicates that virtual synthetics is enabled, as shown in the following:

```
data_domain_user@data_domain_host# ddboost option show
Option          Value
distributed-segment-processing  enabled
virtual-synthetics    enabled
fc                enabled
```

- If upgrading the NetWorker client from a pre-NetWorker 8.1 release to NetWorker 8.1, a Full level backup is required before performing a VSF backup. If the Full level backup is not performed prior to the VSF backup, file-by-file recovery fails.

If all requirements are met and synthetic full backups are enabled, VSF will automatically be performed. If NetWorker detects that one or more of the requirements are not met, then traditional synthetic full mode is used.

If the only missing requirement is that DDR does not have “virtual-synthetics” enabled, NetWorker does not fall back to traditional synthetic full and attempts to perform VSF. In this case, the VSF backup will fail with errors.

## Enable/disable VSF in NMC

VSF is enabled by default and will be performed if all the requirements are met. If you do not want to use VSF, you can disable the option.

### Procedure

1. In the **Administration** window, click **View** and select **Diagnostic Mode**.
2. Click **Configuration**.
3. Select **Groups**.
4. Right-click on the save group for which VSF is to be disabled and select **Properties**.
5. Select the **Advanced** tab in the properties dialog.
6. In the **Operations** pane, uncheck **Perform virtual synthetic full**.

## Performing VSF

Virtual Synthetics are created in the same manner as traditional synthetic full backups by NetWorker commands.

Use one of the following commands:

- `savegrp -l`
- `nsrconsolidate`

### Using the `savegrp` program to perform incremental synthetic full backup

[Performing manual incremental synthetic full backup by using the `savegrp` program on page 81](#) describes how to perform VSF using the `savegrp` program. The procedure for using VSF is the same as traditional synthetic full.

### Using the `nsrconsolidate` command to perform VSF

[Performing manual synthetic full backups using `nsrconsolidate` on page 81](#) describes how to perform VSF using the `nsrconsolidate` command. The procedure for VSF is the same as traditional synthetic full.

## Directives

Directives cannot be used with VSF backups as VSF is created by the Data Domain system.

Directives can still be applied to traditional synthetic full backups, if the VSF option is disabled in NMC.

## Multiple storage node distribution

The VSF save sets backed up from NetWorker Data Domain devices can be distributed across multiple storage nodes.

The following are requirements for distributing multiple storage nodes:

- All of the save sets being used in the VSF are stored on a single Data Domain storage system, and
- The VSF requirements identified in the section [Virtual synthetic full requirements on page 85](#) are met.

Also, save sets located in different mtrees on the Data Domain system can be used in a VSF.

## Concurrent operations

The concurrent volume of Virtual Synthetics that a DDR can handle depends on the DDR model and the capacity of the NetWorker host.

The following scenarios have been tested and verified to work:

- Concurrent VSF
- VSF concurrent with clone
- VSF concurrent with Clone-controlled replication

## VSF validation

There are several methods available to validate VSF backups.

Validate VSF backups using any of the following options:

- `mminfo` commands
- NMC
- `savegrp` logs

### Validating VSF backups

Validate VSF backups by using the `mminfo` command.

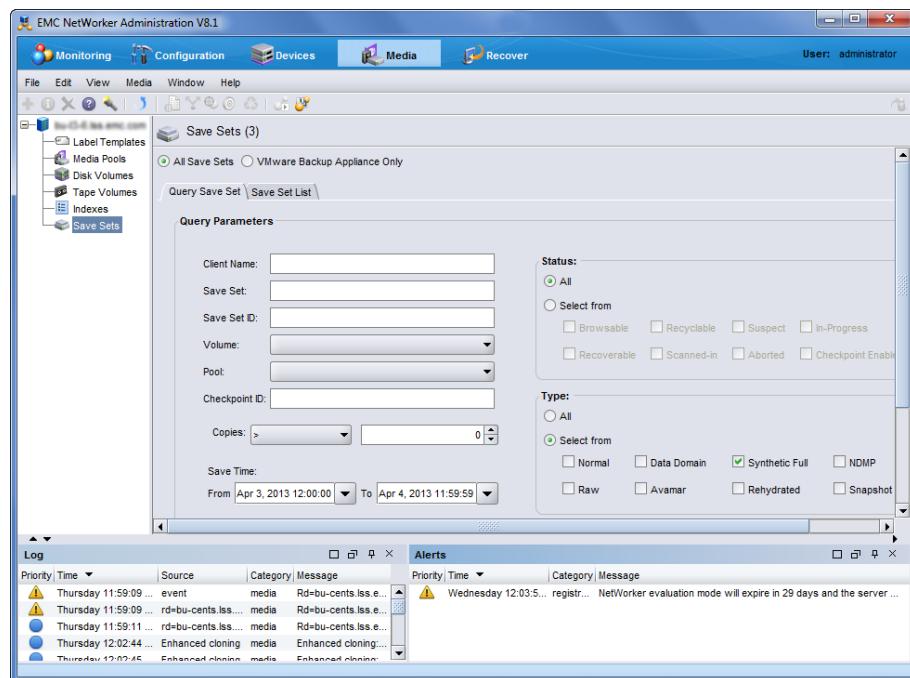
The following table lists the `mminfo` commands with applicable switches.

**Table 16** `mminfo` command for VSF validation

Command with switches	Description
<code>mminfo -aS</code>	Shows detailed information about Synthetic Full backups, including information about the save sets used to form the synthetic full
<code>mminfo -q syntheticfull -c {client} -N {saverset_name}</code>	Queries all synthetic full save sets for the specified client and save set names
<code>mminfo -q rehydrated</code>	Queries rehydrated Avamar save sets
<code>mminfo -avot -q dedupe</code>	Queries all deduplicated Avamar savesets

### Using NMC to validate VSF

[Running queries on synthetic full backups on page 83](#) provides more information.

**Figure 7** Save Sets query in NMC

### Procedure

1. In NMC, query synthetic full backups by navigating to **Media > Save Sets** in the **Administration** window.
2. Select the **Synthetic full** checkbox to return information for all synthetic full save sets.
3. Click **Save Set List**.

### Viewing the savegrp logs to validate VSF

Use savegroup logs to determine the status of attempted VSF backups.

The following excerpts from various savegrp log files illustrate the types of messages NetWorker displays when performing VSF, traditional synthetic full, and falling back from VSF to SF:

```
1707:97864:nsrconsolidate: Unable to perform virtual synthetic full
operation since at least one source save set is an Avamar save set.
Falling back to non-virtual synthetic full mode
1707:97860:nsrconsolidate: Synthetic full save set hostname:/sat-tree
at savetime 1358188522 was created by using non-virtual synthetic mode
95773:nsrrecopy: Virtual synthetic succeeded for hostname:/test1
```

## VSF limitations

There are limitations that apply when using VSF.

Consider the following:

- All DD devices on a storage node must be unmounted prior to upgrading to NetWorker 8.1 if planning to use VSF. If this is not performed, then a new full backup will be required after upgrading and prior to performing any VSF backups.
- DD Archivers must be running DD OS 5.3 or later.
- Cloning fails if the clone device is on a DDR that does not have VSF enabled.

## Enabling parallel save streams

In NetWorker 8.1 and later, the parallel save streams (PSS) feature provides the ability for each Client resource save set to be backed up by multiple parallel save streams to one or more destination backup devices. PSS is used for the scheduled, file-based backup of file systems. PSS is disabled by default. The following table lists the items supported for PSS.

**Table 17** PSS support in NetWorker

NetWorker version	Supported operating systems	Supported save sets	Supported backup types	(Virtual) Synthetic full	Check point Restart
8.1 and Service Packs	UNIX, Linux	ALL, individual save points	Scheduled	No	No
8.2 and Service Packs	UNIX, Linux, Windows	ALL, individual save points including, Disaster_Recovery, deduplicated, and CSV volumes (Windows only)	Scheduled	Yes	No

---

### Note

In NetWorker 8.1 and 8.1 Service Pack 1 there is no PSS support for Synthetic Full, Checkpoint Restart, or Avamar deduplication backups. Also, both the NetWorker server and client must be at NetWorker 8.1 or later to use the PSS functionality for full and incremental level backups, recovery, and cloning.

---

The *EMC NetWorker Performance Optimization Planning Guide* provides complete details on PSS requirements and performance benefits.

### Procedure

1. In **Configuration**, select **Clients**.
2. Right-click the client for which to enable PSS, and select **Modify Client Properties....**
3. In **Globals (1 of 2)**, select the checkbox in the **Optimizations** section to enable **Parallel save streams per save set**.
4. Specify save set **All** or **/paths** in the **Save Set** attribute of the client for which to enable PSS.

## Troubleshooting PSS

It is recommended that you troubleshoot PSS with the guidance of EMC technical support. The *EMC NetWorker Performance Optimization Planning Guide* provides complete details on PSS requirements and performance benefits.

### Procedure

1. Perform the following to enable detailed client logging:
  - Modify the Client resource backup command attribute:

```
save -v -D7
```

- On the client, perform the following command:

```
touch /nsr/debug/mbsdfopen
```

2. Enable the **-v verbose** option for scheduled backups:

```
NMC > Group Properties > Advanced > Options > Verbose > checkbox
```

3. Run the save group, by using any of the following methods:

- NMC:

```
NMC > Group Properties > Setup > Setup > Autostart > Start now
```

- From the server command line:

```
savegrp -v 2>&1 | tee /nsr/tmp/savegrp.log
```

- Wait for the normal automated scheduled group run.

4. After the save group finishes, collect the following log files for EMC technical support:

- Client:

```
/nsr/tmp/save-mbs-* log files
```

- Server:

```
/nsr/logs/daemon.raw log file  
/nsr/logs/sg/<group name>//* log files  
/nsr/tmp/savegrp.log log file
```

## Probe-based backups

You can configure the NetWorker server to search or probe a NetWorker client for a user-defined script, before the start of a scheduled backup operation. A user-defined script is any program that passes a return code.

When the NetWorker server detects the script, the NetWorker server runs the script and interprets two return codes:

- Return code 0: A client backup is required
- Return code 1: A client backup is not required

NetWorker interprets all other return codes as an error during the probe operation and will not perform a backup.

To run a probe-based backup, you must perform the following actions:

- Create the user-defined script.
- Configure a probe-based group
- Create a client probe resource
- Associate the client probe resource with a client.

---

### Note

Users are responsible for creating and supporting user-defined scripts.

## Configuring a probe-based backup group

Add NetWorker clients that will use the probe resource to a NetWorker group that has the Probe attribute enabled.

**Procedure**

1. Create a NetWorker group or modify the properties of an existing group. .
2. On the **Advanced** tab, enable **Probe based group**.

**NOTICE**

If you run the savegrp program with the -g attribute, then the backup operation bypasses the probe operation.

---

## Creating a client probe

Create a client probe resource on the NetWorker server.

Before you create a client probe resource, perform the following tasks:

- Save the probe resource script on each client that will use the client probe, in the same directory as the NetWorker binaries. For example, specify the /usr/sbin for a Solaris or Linux host. The *EMC NetWorker Installation Guide* provides details on default installation paths for all operating systems.
  - Ensure that probe script name begins with save, or nsr.
- 

**Note**

The Command Options field applies to NetWorker Module probes only.

---

**Procedure**

1. From the **NetWorker Administration** window, click **Configuration**.
2. Right-click probes, and select **New**. The **Create NSR probe** window opens.
3. In the **Name:** field, specify the name of the probe.
4. (Optional) In the **Comment** field, specify details for the probe script.
5. In the **Command** field, type the name, and path of the probe script.
6. Associate the probe with a Client resource as described in [Associating a probe with a Client resource on page 91](#).

## Associating a probe with a Client resource

To associate a probe resource with a client, modify the Client resource on the NetWorker server.

---

**Note**

You can associate a probe with each client in a probe-based group but a probe is not required. A probe-based backup group must have at least one probe-enabled client associated with it. If you associate a single probe with multiple clients, make sure that the probe resource script is in the same directory as the NetWorker binaries for each of the clients referencing the probe.

---

**Procedure**

1. From the **NetWorker Administration** window, click **Configuration**.
2. Click **Clients**, and then right-click the client in the **Configuration** screen of the **NetWorker Administration** window.
3. Select **Properties**.

4. On the **General** tab, select the probe-based group.
5. On the **Apps & Modules** tab, select the probe from the **Probe resource name** list. Each defined probe resources appear in the list. [Creating a client probe on page 91](#) describes how to define a probe resource.

## Client Direct backups

The NetWorker 8.0 client software enables clients with network access to AFTD or DD Boost storage devices to send their backup data directly to the devices, bypassing the NetWorker storage node. The storage node manages the devices for the NetWorker clients, but does not handle the backup data. The Client Direct feature reduces bandwidth usage and bottlenecks at the storage node, and provides highly efficient backup data transmission.

Destination devices must specify their complete paths in their Device Access Information attribute. If the Client Direct backup is not available, a traditional storage node backup is performed instead. The Client Direct feature is enabled by default, but can be disabled on each client by the Client Direct attribute.

[Considerations for Client Direct clients on page 165](#) provides details.

## Checkpoint restart backups

The checkpoint restart feature allows a failed backup operation to restart at a known good point, prior to the point-of-failure during the backup. A known good point is defined as a point in the backup data stream where the data is successfully written to the save set and that data can be located and accessed by subsequent recovery operations. This feature allows client backups that are part of a scheduled backup to be restarted, if they fail while running. This prevents the files and directories that have already been backed up from being backed up again.

### Checkpoint restart usage

Backup failures occur for various reasons. The most common reasons include: hardware failures, loss of network connectivity, and primary storage software failures. The NetWorker server and storage node components must remain running to manage the client failure and to create a partial save set. If the NetWorker server or storage node components fail during a backup, partial save sets are not created. In this case, the backup for the checkpoint-enabled client starts from the beginning.

If the checkpoint restart feature is not enabled, a failure encountered during a scheduled backup operation might require a re-run of an entire backup tape set. This can be costly when a limited backup window of time is available, as a significant portion of the backup data might have been successfully transferred to tape, and the NetWorker software cannot resume a save set from the point of interruption.

For example, when performing an 800 GB backup that requires approximately 10 hours to complete and spans 6 tapes, if a failure occurs while writing to the last tape, the previous 5 tapes representing 9 hours of backup time may need to be re-run. As data sets continue to increase in size, so does the impact of backup failures.

Checkpoint-enabled clients provide the following enhancements:

- Failed save sets are marked as partial; not as aborted.
- Restarted save sets have a new SSID and savetime.
- Partial non-NDMP save sets are indexed.

- For partial NDMP savesets, only the first saveset has an index associated with it. The index covers all of the files in all of the partial save sets that make up a complete backup.
- Partial save sets are not removed from the index, the media databases, and media such as AFTD.

## Support and considerations

There are some things to consider when using checkpoint restart configurations.

Consider the following:

- Checkpoint restart is not enabled by default.
- Checkpoint restart does not support Client Direct backups to DD Boost devices. If a client is enabled for checkpoint restart and a Client Direct backup is attempted to a DD Boost device, then the backup reverts to a traditional storage node backup instead.
- Starting in NetWorker 8.0, Checkpoint restart does not support Avamar deduplication backups.
- Checkpoint restart does not support NDMP NetApp clients for releases earlier than NetWorker 8.0 server and client software. [NetWorker support for NDMP on page 551](#) provides details.
- Checkpoint restart does not support NDMP Isilon clients for releases earlier than the NetWorker 8.1 SP1 server and client software. [NetWorker support for NDMP on page 551](#) provides details.
- Checkpoint restart for non-NDMP clients is not supported for releases earlier than NetWorker 7.6 SP1 server and client software.
- Backup of the Windows DISASTER\_RECOVERY:\ save set is not supported. If a client with a DISASTER\_RECOVERY:\ save set is enabled for checkpoint restart, the backup fails. [Save sets on page 68](#) provides details.
- For Client Direct backups to AFTDs, checkpoints are not made less than 15 seconds apart. Checkpoints are always made after larger files that require more than 15 seconds to back up.
- The checkpoint restart option is ignored for index and bootstrap save sets.
- Checkpoint-enabled might impact the backup speed. This depends on the datazone environment and configuration.

Using the checkpoint restart feature might increase the size of the index. This increase might occur because additional index records are created for the valid recoverable data. These partial save sets should not be manually removed from the index.

## About partial non-NDMP save sets

The backup sequence of partial save sets is not the same as for complete backups. Each partial save set provides protection for a part of the filesystem, but the completeness and consistency of the coverage of the whole filesystem cannot be guaranteed.

The checkpoint restart window is user-defined and can be large. If restarted hours apart, the partial backups might provide an image of the filesystem that is different from the state of the filesystem at any given point-in-time. The resulting filesystem is not guaranteed to be consistent. It can be different than at any other point-in-time.

Files and directories are backed up in alphabetical order. If a crash occurs, subsequent backups continue from the last point alphabetically from where they were in progress. Previously backed up files or directories are not reviewed for modifications. If a file or directory that is earlier alphabetically was modified or added, it will not be backed up.

### Example

A backup is interrupted while saving a directory and restarted after the directory contents have changed. As a result, different files are saved than the original filesystem entry.

1. A save set contains `/disk1/dir`. The files include `file_a`, `file_c` and `file_d`.
2. A point of interruption occurs in the backup of the save set when `file_d` is being backed up.
3. The first partial save set contains `file_a` and `file_c`.
4. Before the checkpoint restart is initiated for the save set, `file_b` is added to the filesystem.
5. The second partial save set contains `file_d` and `/disk1/dir`.

**NOTICE**

---

`/disk1/dir` contains `file_a`, `file_b`, `file_c`, and `file_d`.

---

6. Notice that `file_b` has not been backed up.

## About partial NDMP save sets

For checkpoint enabled backups of an NDMP client, the NetApp filer creates a snapshot of the filesystem prior to the start of the backup. The save set is generated from the snapshot. If the NDMP backup is interrupted and later restarted, the partial save sets are generated from the snapshot. As a result, the partial backups provide an image of the filesystem from the point-in-time that the snapshot is taken.

## Configuring checkpoint enabled clients

NetWorker clients can be configured to allow an interrupted backup to restart from the point-of-failure.

Consider the following:

- For non-NDMP save sets the backup can be restarted at the directory or file level from the point of failure. The level is defined by the Checkpoint Granularity attribute for the client.
- For NDMP save sets, checkpoints are made at regular time intervals during the backup. The interval is set by an environment variable defined in the Application Information attribute for the client. The backup is restarted from the last successful checkpoint.
- The checkpoint restart feature is not enabled by default.
- Configuring a client as checkpoint enabled might impact the backup speed. This is dependent upon the data zone environment and its configuration.
- Ensure that all NetWorker clients are configured with the same name. There should not be both short and fully qualified domain name (FQDN) client resources. [Hostname aliases on page 684](#) provides more information.

### Procedure

1. From the **Administration** window, click **Configuration**.
2. Set the **Checkpoint enabled** attribute:
  - a. In the expanded left pane, select **Clients**.
  - b. Right-click the client to be enabled.

- c. Select **Properties**. The **Properties** dialog box appears.
  - d. Click the **General** tab.
  - e. Click the **Checkpoint enabled** checkbox.
3. For the **Checkpoint granularity** attribute:
- a. Select whether to restart the backup **by directory or by file**. This value is not applicable to NDMP clients and will be ignored.  
Restart by directory is the default. After each directory is saved, the data is committed to the media and index database. If a directory contains a large number of entries, intermediate checkpoints are created.  
Use the restarting by file option only for save sets with few large files. Committing every file to the index and the media database is time consuming. This might lead to performance degradation during a backup that contains many small files.
  - b. Click **OK**.
4. For NDMP NetApp clients only, define the interval at which checkpoints are written during the backup using the *CHECKPOINT\_INTERVAL\_IN\_BYTES* variable. This variable is added to the **Application Information** attribute located under the **Apps and Module** tab.
- The value defined for *CHECKPOINT\_INTERVAL\_IN\_BYTES*:
- Is in bytes by default.  
For example: *CHECKPOINT\_INTERVAL\_IN\_BYTES*=1000000
  - Can be defined using different multipliers. Acceptable multipliers include: KB, MB, GB, TB, kb, mb, gb, and tb.  
For example: *CHECKPOINT\_INTERVAL\_IN\_BYTES*=1GB
  - Is automatically rounded up to a multiple of the tape blocksize.
5. Select the group to which the checkpoint enabled client belongs:
- a. In the expanded left pane, select **Groups**.
  - b. Click the **Advanced** tab.
  - c. If required, change the **Client Retries** attribute to a value greater than 0. This value specifies the number of times the NetWorker software attempts to back up a failed client.
  - d. Click **OK**.

## Restart checkpoint-enabled backups

Restarting a checkpoint-enabled backup of a partial save set is faster than restarting the backup of a save set from the beginning. This depends on how much data was saved in the previous backup.

There are two ways in which a checkpoint-enabled backup can be initiated:

- Manually through a group restart operation.
- Automatically by setting the Client retries attribute in the Group resource of the checkpoint-enabled client.

**NOTICE**

Changing the name of a save set will cause checkpoint restart to fail to find a match against a previous run, and the restart will revert to a complete backup. Additionally, do not modify browse or retention policies for the client in between checkpoint restarts, as an expired partial save set may leave gaps in the backup set.

## Manually restarting a checkpoint enabled backup by using the Group Restart attribute

When a Group is restarted, the NetWorker software determines which save sets were not completed within the backup:

- If the client is Checkpoint-enabled, the incomplete save sets are checkpoint restarted and continue from the point at which they were stopped.
- If the client has not been checkpoint-enabled, the incomplete save sets are backed up again in full.

### Procedure

1. Ensure that the client has been checkpoint-enabled.
2. From the **Administration** window, click **Monitoring**.
3. Click **Groups** in the docking panel.
4. Right-click the group to which the checkpoint enabled client belongs, then select **Restart**.
5. Click **Yes** to confirm the restart.

## The Client retries attribute

If the NetWorker server fails to connect to a client, the Client retries attribute specifies the number of times that the server will reattempt the connection to the client before the backup is considered a failure. The Client retries mechanism is the same for checkpoint-enabled clients and non-checkpoint enabled clients, with the exception that a partial save sets is created when there is a failure for a checkpoint-enabled client.

If the NetWorker software detects that the backup fails and the number of client retries is not exceeded, the NetWorker software will checkpoint-restart the backup, immediately after the failure. This operation takes into account the Group restart window and will not restart the backup if the defined backup window has expired.

### Example 1:

There are 6 clients in a group, each with 3 save sets. The Client retries attribute for the group is 1. One save set fails and it is checkpoint restarted immediately. The remaining save sets in the group continue to backup. The save set fails a second time. A checkpoint restart for the save set does not occur because the retry attempt would exceed the value that is defined in the Client retries attribute.

When all of the save set backup attempts in the group complete, the group completion report:

- Provides a list of the successful save sets.
- Reports that the failed partial save set is unsuccessful.
- Reports that the group has failed.

### Example 2

There are 6 clients in a group, each with 3 save sets. The Client retries attribute for the group is 2. One save set fails and it is checkpoint restarted immediately. The remaining save sets continue to backup. The partial save set fails a the second time and it is checkpoint restarted immediately. This time, the partial save set succeeds.

When all of the save set backup attempts in the group are complete, the group completion report:

- Provides a list of the successful save sets.
- Reports that the two partial save sets are successful.
- Reports that the group completed successfully.

To increase the number of times each client in a group is retried before the backup attempt is considered unsuccessful, change the value in the Client retries attribute in the Group resource.

## Monitoring checkpoint-enabled backups

You can view detailed information about a checkpoint-enabled backup.

### Procedure

1. From the **Administration** window, select **Monitoring > Groups**.
2. Right-click the group to which the checkpoint enabled client belongs, then select **Show Details**.
3. View the detailed information related to the group backups:
  - If the partial save set is in the work list for the group, the save set appears in the **Waiting to Run** section.
  - If the partial save set is running, the save set appears in the **Currently Running** section.
  - If the entire partial save sets sequence of the savegroup is complete, the save set appears in the **Completed Successfully** section.
  - If the entire partial save sets sequence of the savegroup is not complete, the save set appears in the **Failed** section.

**NOTICE**

If any messages are generated, the Show Messages button is enabled. Click Show Messages to view the messages.

4. Click **OK** to close the **Group Details** window.

## Checkpoint-enabled backup reporting

The daemon.raw file on the NetWorker server contains details about groups that are run with checkpoint-enabled clients. When a group backup complete, the savegroup completion report also reports the status of each client backup.

### View the savegroup reports for checkpoint-enabled client backups

There are several things to consider when reviewing the savegrp completion report for a savegroup that contains a checkpoint-enabled client.

- When a checkpoint-enabled client backup attempt fails:
  - The savegroup status is reported as a failure:

```
nsrd info, savegroup failure alert: test Completed/Aborted,
Total 1 client(s), 0 Clients disabled, 0 Hostname(s)
Unresolved, 0 Failed, 0 Succeeded, 1 CPR Failed, 0 CPR
Succeeded, 0 BMR Failed, 0 BMR Succeeded.
nsrd info, savegroup alert: <group_name>aborted, Total 1
```

```
client(s), 1 CPR Failed. Please see group completion details
for more information.
```

- The failed save sets are reported in the **Unsuccessful Save Set** status section:

```
* cprclient.emc.com:/usr/sbin, number of checkpoint enabled
savesets 1
* cprclient.emc.com:/usr/sbin 86705:save: Successfully
established DFA session with adv_file device for save-set ID
'4078798790' (bu-t3-7.lss.emc.com:/usr/sbin).
* cprclient.emc.com:/usr/sbin (interrupted), exiting
* cprclient.emc.com:/usr/sbin aborted
```

- When a checkpoint-enabled client backup succeeds:

- The savegroup status is reported as a success:

```
NetWorker savegroup: (notice) test completed, Total 1
client(s), 1 CPR Succeeded. Please see group completion details
for more information.
```

- The total number of partial save sets that make up the checkpoint save sets is displayed in the **Save Set Summary** section:

```
client_name:save_set, number of checkpoint enabled savesets x
```

- The failed save sets are reported in the **Successful Save Set** status section:

```
* cprclient.emc.com:savefs savefs cprclient.emc.com: succeeded.
bu-t3-7.lss.emc.com:/usr/sbin, number of checkpoint enabled
savesets 2
* cprclient.emc.com:/usr/sbin 86705:save: Successfully
established DFA session with adv_file device for save-set ID
'4062021648' (bu-t3-7.lss.emc.com:/usr/sbin).
```

## Determine the status of a checkpoint-enabled backup

Review the daemon.raw file on the NetWorker server to determine the status of a checkpoint-enabled client backup.

```
nsrd info, Savegroup Info: group_name:client_name checkpoint enabled,
mode: mode. (severity 0, message 71193)
```

This message is reported when a savegroup is started. This message reports the names of the clients that are checkpoint-enabled, and the mode that was selected at the time of the backup.

savegrp test: checkpoint restartable saveset client\_name:save\_set created in previous run(s) of the group. It will be checkpoint restarted. Checkpoint ID cp\_id

This message reports that a partial save set is detected for a client in the group and a checkpoint restart will occur for the save set.

savegrp group\_name checkpoint restartable saveset client\_name:save\_set failed and will not be restarted

This message is reported when the backup of a checkpoint-enabled client fails and the backup will not be retried.

Common reasons for this error message include:

- The Restart window for the group has been exceeded.
- The maximum number of Client retries has been reached.

**NOTICE**

When this message is reported, the failed save set are removed from an AFTD: nsrd info, MeDia Info: save set save\_set for client client\_name was aborted and removed from volume volume\_name (severity 0, message 71193)Recovering data.

---

savegrp group\_name: checkpoint restartable saveset client\_name:save\_set completed without interruption

This message reports that the save set for a checkpoint-enabled client successfully completed during the group backup.

## Query the media database for partial save sets

The savegrp completion report does not provide detailed information about partial save sets that might be necessary to perform a recovery.

### Querying partial save sets from the Console

You can view information about the partial save sets by using the NetWorker Console.

**NOTICE**

If no partial save sets are found that match the query, ensure that the backup of the partial save sets was started within the Save Time period. To change the values for the Save Time attribute, open the Save Set Query tab and select a date and time from the Save Time calendar.

#### Procedure

1. In the **Administration** window, click **Media**. Media-related topics appear in the navigation tree.
2. Select **Save Sets**. The following tabs appear in the **Save Sets** window:
  - **Query Save Set**
  - **Save Set List**
3. Select the **Query Save Set** tab, to query:
  - All partial save sets, select **Checkpoint Enabled**.
  - All partial save sets with the same Checkpoint ID, in the **Checkpoint ID** field, type the **Checkpoint ID** of the partial save set on which you want to perform the query.
4. Select the **Save Set List** tab to view the result of the save set query:
  - The **Checkpoint ID** column displays the partial save set **Checkpoint ID** and its Sequence ID. The **Checkpoint ID** is listed first followed by the **Sequence ID**, which is encased within brackets.
  - Sort the **Checkpoint ID** column to view the complete sequence of partial save sets.
  - The **Status** column displays the status of the partial save sets:
    - A Checkpoint browsable status indicates that the save sets can be browsed for recover.
    - A Checkpoint aborted status indicates that the backup of the partial save set was stopped or aborted. A save set recover is used to recover the partial save set.
  - Consider the following:
    - When a checkpoint-enabled backup completes successfully, the status of the last partial save set is Checkpoint browsable.

- When a checkpoint-enabled backup completes successfully, on the first backup attempt, the save set status is Checkpoint browsable. Only one Sequence id is associated with the Checkpoint ID. The Sequence id is 1. If the Sequence id is 2, the first partial save set in the checkpoint-enabled backup is missing.

## Querying partial save sets by using the `mminfo` command

By default, the `mminfo` command output only displays the browsable save sets. The first and intermediate partial save sets are not displayed. Only complete checkpoint-enabled save sets or final partial save sets are displayed.

Use the `mminfo` command with specific queries to display more information about checkpoint-enabled save sets.

The following table lists the new media attributes support the Checkpoint Restart feature.

**Table 18** New Checkpoint Restart media attributes

Media attribute	Description
<code>checkpoint_id</code>	Displays the checkpoint restart id of the partial save set in the <code>chkpt_id</code> column
<code>checkpoint_seq</code>	Displays the partial save set sequence id in the <code>chkpt_seq</code> column
<code>checkpoint-restart</code>	This flag attribute is used to only display checkpoint restart enabled save sets

In addition, several media sumflags are used with the Checkpoint Restart feature:

- `k` — Indicates this is a checkpoint enabled save set.
- `a` — The first and all intermediate partial save sets of a checkpoint sequence will have aborted status.
- `b` — The last partial or complete save set of a checkpoint sequence will be marked browseable.

## Displaying checkpoint enabled save sets

Display all checkpoint enabled save sets by using the following `mminfo` command:

```
# mminfo -q 'checkpoint-restart' -r 'client,nsavetime,ssid(11),sumflags(3),name,checkpoint_id,checkpoint_seq'
```

client	save time	ssid	ssflags	filename	chkpt_id	chkpt_seq
plapew	1251910303	4204700319	cak	/space	1251910303	1
plapew	1251910327	4187923127	cbk	/space	1251910303	2
plapew	1251910710	4087260214	cak	/space	1251910710	1
plapew	1251910725	4070483013	cbk	/space	1251910710	2

## Displaying all partial save sets for the checkpoint id

Display all partial savesets for the checkpoint id by using the following `mminfo` command:

```
mminfo -q "checkpoint_id=1251910303"
```

volume	client	date	size	level	name
plapew.001	plapew	09/02/09	17 MB	full	/space
plapew.001	plapew	09/02/09	799 MB	full	/space

## Checkpoint restart data recovery

This section outlines how to recover data in the following two scenarios:

- [Recovering data from the complete sequence of partial backups that comprise the original save set on page 101](#)
- [Recovering data from a partial save set on page 101](#)

### Recovering data from the complete sequence of partial backups that comprise the original save set

File-by-file recover is available only if there is a complete sequence of partial save sets that span the original save set. The directory structure is saved after the files are saved. If the directory structure is not available, then the browser cannot access the files.

You can restore data from the complete sequence of partial save sets that make up the original save set.

#### NOTICE

If the sequence of partial save sets is incomplete and does not make up the original save set, use the save set recovery procedure to recover the data from the partial save set.

#### Procedure

1. Perform a query for all partial save sets. [Querying partial save sets from the Console on page 99](#) provides detailed information.
2. Use one of the following programs to restore the data:
  - For Windows - The NetWorker User program
  - For UNIX - The recover program

### Recovering data from a partial save set

Recovering from a partial NDMP save set differs from a non-NDMP save set.

The following lists the differences:

- A save set recovery of a partial NDMP save set, recovers all of the partial save sets in the checkpoint sequence. The data in a partial save set cannot be recovered independently of the other partial savesets in the checkpoint sequence.
- A save set recovery of a non-NDMP save set enables you to recover data from a partial save set rather than by broWindows Searchng and selecting individual files for recovery. However, the partial save set only contains successfully backed up files and not the entire set of data. An incomplete set of partial save sets cannot be browsed.

The procedure to restore data from partial save sets is the same as recovering by save set selection. [Overview of NetWorker recovery methods on page 351](#) provides detailed information on performing data recovery.

Use the `nsrinfo` command to display the contents of a partial save set.

The `nsrinfo` man page or the NetWorker 8.0 Command Reference Guide provides detailed information about the `nsrinfo` command.

## Partial saveset cloning and scanning

Partial save sets can be cloned and scanned individually. These operations must be performed on every partial save set.

If legacy automatic cloning is enabled, all partial save sets are cloned because automatic cloning is run as part of the scheduled backup.

## Cloud backup devices and partial savesets

By default, the CheckPoint restart feature does not support cloud backup devices because partial save sets are not retained on cloud backup devices.

### Retaining partial save sets on a cloud device workaround

When the cloud backup device is used as a backup device for a Checkpoint restart operation, you can keep partial save sets by using a workaround.

Enable the Keep Incomplete Backups attribute on the Server Properties menu.

If the Keep Incomplete Backups attribute is not enabled, the NetWorker software will not keep the partial savesets.

## Deduplication backups

The *EMC NetWorker Avamar Integration Guide* provides more information about Avamar deduplication backups.

The *EMC NetWorker Data Domain Deduplication Devices Integration Guide* provides information on DD Boost deduplication backups using Data Domain storage systems.

## Backup data encryption

Backup and archive data on UNIX and Windows hosts can be encrypted with the aes Application Specific Module (ASM). The aes ASM provides 256-bit data encryption. Backup data is encrypted based on a user-defined pass phrase. If no pass phrase is specified, data is encrypted with a default pass phrase.

## Microsoft Encrypting File System (EFS) and NetWorker AES encryption

Do not use NetWorker AES data encryption when backing up files that are encrypted by using the Microsoft Windows Encrypting File System (EFS). Even though the backup will be reported as successful, recovery of the file will fail and the following message will be written to the NetWorker log file: recover: Error recovering <filename>. The RPC call completed before all pipes were processed.

When EFS encrypted files are backed up, they are transmitted and stored on backup volumes in their encrypted format. When they are recovered, they are also recovered in their encrypted format.

## Setting the Datazone pass phrase for a NetWorker server

### NOTICE

By default, the current Datazone pass phrase is automatically used to recover password-protected files. If the current Datazone pass phrase was created after a password-protected backup was performed, you must provide the password that was in effect when a file was originally backed up. Keep password changes to a minimum.

### Procedure

1. From the **Administration** window, click **Configuration**.
2. Select the server name.
3. From the **File** menu, select **Properties**.
4. Click the **Configuration** tab and type a pass phrase in the **Datazone pass phrase** attribute.
5. Click **OK**.

## Apply AES data encryption to clients in the datazone

To implement AES data encryption. Apply the Encryption global directive to individual clients by using the Directives attribute of the Client resource.

## Backup data compression

Compressing data for a backup generates less network traffic. However, compression uses computing resources, so its benefits may be limited on low-powered systems. If the storage device also compresses data, the result may be that more data is actually written to tape.

### NOTICE

Both compression and password-protection cannot be selected.

## Applying compression to a scheduled backup

There are 2 methods available to apply compression to a scheduled backup.

- Use the compressasm ASM in a local or global directive to apply compression to a scheduled backup.
- Use a preconfigured directive that is appropriate for the client computer operating system.

## Applying compression to a manual backup

You can compress data for a manual backup on Windows. To compress data for a manual backup on UNIX, you must use the compressasm in a local directive file.

### Procedure

1. Open the **NetWorker User** program and click **Backup**.

2. Mark the data to be compressed.
3. From the **File** menu, select **Special Handling**.

## Handling data for NetWorker clients on Windows

You can select directories and files for password-protection, encryption, and compression, or you can clear selected data items.

### Procedure

1. In the **NetWorker User** program, click **Backup**.
2. In the **Backup** window, select each data item to be designated for compression, encryption, or password-protection. If you select a disk volume or directory for an operation, the special handling will be applied to all of its nested subdirectories and files.
3. From the **File** menu, select **Special Handling**.
4. Select an option and click **OK**. You can also right-click the file and select a special handling options.

Depending on which special handling options were selected, the letter P (password-protection), E (encryption), or C (compression) appears next to the folder or filename.

5. Remove special handling by selecting a data item, and clicking **Remove**.

## Console server management data backups

To protect the Console server management data, such as report information, perform regular backups of the Console server database. The Console server database remains available during the backup.

### NOTICE

The `savepsm` backup command backs up the Console server database and also backs up the database credential file and the authentication configuration files in a separate save set named `CONSOLE_BACKUP_FILES`.

## Scheduling backups for the Console server database

If a NetWorker server was specified during the setup of the Console server in the Console Configuration Wizard, a Client resource was created to back up the Console server database on a scheduled basis. If a Client resource was created, modify the Client resource with respect to the backup schedule, browse and retention policies, and so on.

If a Client resource was not created to back up the Console server database, create a Client resource.

### NOTICE

Only full, incremental, and skip backup levels are supported. All other backup levels (1-9) are mapped to an incremental backup.

### Procedure

1. From the **Console** window, click **Setup**.
2. From the **Setup** menu, select **Set Database Backup Server**.
3. In the **NetWorker server** attribute, type the name of the NetWorker server that will back up the Console server database.

4. Select the **Create client** resource.
5. In the **Client name** attribute, type the name of the Console server.
6. Click **OK**.

A Client resource is created with the following attributes:

- **Name** attribute: the name of the Console server computer.
- **Save Set** attribute:

**NMCASA:/gst\_on\_server\_name/lgtogst**

where <server\_name> is the short name of the host where the Console server component was installed.

- **Backup Command** attribute: **savepsm** (for a Windows Console server) or **savepsm.sh** (for a UNIX Console server).

One can also specify a NetWorker server to back up the Console server database through the Console Configuration Wizard.

## Performing a manual backup of the Console database

Before performing a manual backup on UNIX, set the appropriate library path environment variable to:

- **Console\_install\_dir/sybasa/lib64**
- **Console\_install\_dir/sybasa/lib** on Linux

The environment variable to set varies by platform:

- Solaris/Linux: **LD\_LIBRARY\_PATH**
- AIX: **LIBPATH**

Perform a manual backup of the Console server database by using the following **savepsm** command:

```
savepsm -I "Console_install_dir" save options
```

where **Console\_install\_dir** is the installation directory for the Console server.

Example:

- On Solaris, the default installation directory is **/opt/LGTONmc**
- On Linux/AIX, the default installation directory is **/opt/lgtomc**
- On Windows, the default installation directory is **C:\Program Files\EMC NetWorker\Management\GST**

Installation directory paths that have spaces must be enclosed in quotations. For example:

```
savepsm -I "C:\Program Files\EMC NetWorker\Management\GST" save options
```

The *EMC NetWorker Command Reference Guide* or the UNIX man pages provides information about the **savepsm** command.

## Managing the size of the Console database log file

The Console database transaction log files are automatically truncated whenever a scheduled or a manual backup of the Console server database is performed.

Truncate the transaction log file without performing a backup by using the following savepsm command:

```
savepsm -I "<Console_install_dir>" -T
```

### Managing the Console database log file

If the transaction log file is truncated manually, the next Console server database backup that is performed after truncation must be a full backup. The next backup can be either a scheduled backup or a manual backup.

You can ensure that the next scheduled backup of the Console server database is a full backup.

#### Procedure

1. Open the backup schedule for the Client resource that is associated with the Console server database.
2. If necessary, perform a manual override on the next scheduled backup so that it is a full backup. When performing a manual backup, a full backup is performed by default.

## Windows mount point back ups

A volume mount point (or mount point) is an NTFS file system feature of Windows 2008 and Windows 2008 R2.

Assigning a drive letter to a mount point is optional. Many disk volumes can be linked into a single directory tree, with a single drive letter assigned to the root of the host volume.

#### NOTICE

NetWorker backup and recovery of mount points require special handling, as explained in this section.

### Including mount points in scheduled backups

Specify the host volume, and each mount point to include mount points and their data in scheduled backups.

For example, to back up a single mount point on drive D: and all of its data, include this in the client's Save Set attribute:

D:\mountpoint\_name

Include nested mount points in scheduled backups by doing either of the following:

- Specifying save set All
- Specifying the host volume and the full path to each mount point.

For example, to back up three nested mount points and their data on drive D:, include these in the client's Save Set attribute:

```
D:\mountpoint_name1
D:\mountpoint_name1\mountpoint_name2
D:\mountpoint_name1\mountpoint_name2\mountpoint_name3
```

## Performing a manual backup of a mount point and its data

### Procedure

1. Start the **NetWorker User** program.
2. Click **Backup**.
3. In the **Backup** window, expand the host drive that contains the mount point to back up, for example, drive D:\.
4. Under D:\, select the mountpoint\_name.
5. Expand the mountpoint\_name and verify that all data beneath it is selected for backup.
6. Click **Start**.

## Performing a manual backup of nested mount points and their data

You can perform a manual backup of nested mount points and their data by performing successive backup operations for each nested mount point and its data.

Use the **NetWorker User** program to back up three nested mount points and their data on drive D:\.

### Procedure

1. Start the **NetWorker User** program.
2. Back up the top-level mount point and its data:
  - a. Click **Backup**.
  - b. In the **Backup** window, expand drive D:\ and mark mountpoint\_name1.

#### **NOTICE**

When you mark a mount point for backup, all files, directories, and nested mount points beneath it are marked by default. Before starting the backup, make sure only mountpoint\_name1 and the files and directories beneath it are marked. You must unmark any mount points nested beneath mountpoint\_name1.

- c. Click **Start** to run the backup.
3. Back up the second mount point and its data:
  - a. Click **Backup**.
  - b. In the **Backup** window, expand D:\ and *mountpoint1*.
  - c. Select *mountpoint\_name2* and its data.

#### **NOTICE**

Be sure to clear (unmark) any mount points nested beneath *mountpoint\_name2* before starting the backup.

- d. Click **Start** to run the backup.

4. Back up the third mount point and its data:
  - a. Click **Backup**.
  - b. In the **Backup** window, expand D:\, then expand *mountpoint\_name1*, then expand *mountpoint\_name2*.
  - c. Select *mountpoint\_name3* and its data.
  - d. Click **Start**.

## Windows Content Index Server or Windows Search Index backups

The Windows Content Index Server (CIS) on Windows 2008 and Windows Search Index services index the full textual contents and property values of files and documents stored on the local computer. The information in the index can be queried from the Windows search function, the Indexing Server query form, or a web browser.

### Back up CIS or Windows Search on Windows

The backup and recovery of the CIS or Windows Search occurs as part of the WINDOWS ROLES AND FEATURES component of the DISASTER \_RECOVERY:\ save set. The CIS or Windows Search is automatically regenerated upon system reboot.

#### NOTICE

Back up the DISASTER \_RECOVERY:\ save set whenever you create, move or rename the CIS or Windows Search databases.

Before a CIS or Windows Search backup, the NetWorker software performs the following:

- Pauses any CIS or Windows Search catalogs that are to be backed up.
- Backs up all files that belong to those catalogs.
- Turns the catalogs on again when the backup is finished. A catalog can still be queried when it is paused, so the indexing functionality is not lost during the CIS or Windows Search backup.

CIS or Windows Search deletes the catalog folder during a backup and restores it as part of a recovery operation.

### CIS or Windows Search backup problem troubleshooting

You can troubleshoot problems with a CIS Windows Search backup by using several methods.

Use any of the following troubleshooting methods:

- For CIS, ensure that the catalog folder is named catalog.wci.
- Restart the CIS or Windows Search service.
- Ensure that the CIS or Windows Search service was installed correctly.
- Pause or stop the catalogs, and then try the backup again.

## Directing NetWorker software to skip CIS or Windows Search catalog backups

Skip a CIS or Windows Search catalog backup by creating or modifying an existing Directive resource in the NetWorker Console, and excluding the appropriate file.

- For CIS, exclude the catalog.wci folder. For example, add the following lines a new directive resource:

```
<< / >>
+skip: catalog.wci
```

- For Windows Search, exclude the windows.edb file. For example, add the following lines a new directive resource:

```
<< / >>
+skip: windows.edb
```

---

### Note

In a new directive resource, leave the first line intentionally blank.

---

## Backing up Windows DHCP and WINS databases

The WINDOWS ROLES AND FEATURES component of the DISASTER\_RECOVERY:\ save set contains the Windows Dynamic Host Configuration Protocol (DHCP) and Windows Internet Naming Service (WINS) databases. Use Windows BMR recovery to perform an offline restore of these database.

The ALL save set automatically includes the DHCP and WINS databases. If you do not specify the ALL save set in the Save set attribute for the client, perform the following steps ensure that you include the databases as part of a filesystem backup:

- Manually back up a DHCP database by including the following directory in the Save set attribute for the NetWorker client that is the DHCP server: %SystemRoot%\System32\dhcp
- Back up a WINS database by using the Microsoft WINS administrative tools:
  - Configure an automated backup of the WINS database to a local drive on the WINS server.
  - Ensure that you include the location chosen in the previous step in the save set attribute for the NetWorker client that is the WINS server.  
The Microsoft documentation provides information about the Microsoft WINS administrative tools.

## Windows backup and recovery notes

There are many considerations for the backup and recovery of data on Windows clients.

### Enabling short filename support

NetWorker software provides backup and recovery support for the short filenames that are automatically assigned by the Windows filename mapping feature. Windows filename mapping is an operating system feature in which each file or folder with a name that does not conform to the MS-DOS 8.3 naming standard is automatically assigned a second

name that does. For example, a directory named Microsoft Office might be assigned a second name of MICROS~2.s

Support for short filenames is disabled by default to improve performance.

#### Procedure

1. From the **Administration** interface window, click **Configuration**.
2. In the left pane, click **Clients**.
3. Right-click the appropriate client and select **Properties**.
4. Click the **Globals (2 of 2)** tab.
5. Select the **Short filenames** attribute.
6. Click **OK**.

## Enabling hard link support on a NetWorker client

The NetWorker server backs up and recovers files with hard links. However, the hard links of files created by using a Portable Operating System Interface (POSIX) application are not preserved during recovery.

Support for hard links is disabled by default to improve performance.

#### Procedure

1. From the **Administration** window, click **Configuration**.
2. In the left pane, click **Clients**.
3. Right-click the appropriate client and select **Properties**.
4. Click the **Globals (2 of 2)** tab.
5. Select the **Hard links** attribute.
6. Click **OK**.

## Failed backup and recovery attempts

The NetWorker log file, located in <install\_path>\logs\networkr.raw, contains a record of every file that was part of an attempted manual backup or recovery that was performed from the NetWorker User program. This file is overwritten with the next manual backup or recovery. If the file contains information that should be saved, you should rename the file or export the information by using the nsr\_render\_log program.

## Granting full permissions for backup of Disk Quota database

NetWorker software backs up and recovers the Windows disk quota database as a component of the WINDOWS ROLES AND FEATURES save set. For any NetWorker client that uses the Windows Disk Quota feature, during WINDOWS ROLES AND FEATURES backup, NetWorker software creates temporary files to store the disk quota database settings in the root directory of each drive on the client.

If the permission settings for a local drive do not allow full control to the local system account, the disk quota database backup fails and an error message, similar to this, appears:

```
Failed to write to quota file, 0x80070005
```

**NOTICE**

By default, everyone has full permissions. If that setting has been changed such that the system account does not have full permissions, you must grant full permissions to the system account in order for the disk quota database to be backed up. For more information on setting permissions, refer to the Microsoft Windows documentation.

**Procedure**

1. Log in with administrator privileges to the NetWorker client host computer.
2. Using **Windows Explorer**, perform these steps for each local drive:
  - a. Right-click a drive icon.
  - b. In the **Properties** dialog box, select the **Security** tab.
  - c. Make sure the permissions settings allow full control to the system account.

## Native VHD volume support

NetWorker supports mounted, native VHD volumes on Windows 7, Windows 8, Windows 8.1, Windows Server 2008 R2, Windows Server 2012 and Windows Server 2012 R2. The VHD or virtual hard disk, is used as a mounted volume on designated hardware without any other parent operating system, virtual machine, or hypervisor. The volume can be used as a boot volume or as a data volume.

NetWorker has the following restrictions when using mounted, native VHD volumes:

- Native VHD volumes are not included in the ALL save set. You should configure a separate scheduled client to backup any native VHD volumes.
- Native VHD volumes should not be used as critical volumes if the volume that contains the native VHD is also a critical volume. This situation creates a conflict during a Windows Bare Metal Recovery backup.

## Avoiding recovery problems with case-sensitivity

The NetWorker server is case-sensitive with regard to backup and recovery, although Windows file systems are not case-sensitive. This may result in the creation of multiple files with the same name but different cases.

For example, if you back up a file that is named temp.txt, delete it, then create a new file named Temp.txt, and then recover the old file, you will have two identical files in the directory -- one named temp.txt and the other named Temp.txt.

Avoid problems that result from case sensitivity by disabling POSIX compliance by setting the following system environment variable: *NSR\_DISABLE\_POSIX\_CREATE=YES*

The Windows online help contains detailed instructions about setting system environment variables.

## Enabling NetWorker logging operations performed by backup operator

By default, members of the Windows Backup Operators group do not have write permission to the <NetWorker\_install\_path>\logs directory.

NetWorker log operations are performed by members of the Windows Backup Operators group.

Enable NetWorker logging for Backup Operators by modifying the security settings on the <NetWorker\_install\_path>\logs directory. For example:

### Procedure

1. In **Windows Explorer**, navigate to the <NetWorker\_install\_path>\logs directory.
2. Right-click the <NetWorker\_install\_path>\logs directory icon and select **Properties**.
3. On the **Security** tab of the **Properties** dialog box, add the **Backup Operators** group to the list of groups and users.
4. Select the **Backup Operators** group and click **Allow Write**.
5. Click **OK**.

## Customizing the backup command

You can customize client backups by creating additional programs (scripts) that affect the way the NetWorker server backs up client file system data. For example, one can create a program that performs the following:

### Procedure

1. Shuts down a mail server or database before the NetWorker server performs a backup operation.
2. Restarts the mail server or database after the backup has completed.
3. Prints a message, such as, “Backup started at 3:33 A.M.”
4. Runs the backup.
5. Prints a message, such as “Backup completed at 6:30 A.M.”

Customize a client’s scheduled backups in either of two ways:

- By creating a script that invokes the **save** program as part of its instructions. When the client is backed up, the customized program is invoked instead of the standard **save** program.
- By typing **savepnp** in the Backup Command attribute of the Client resource. This way, the client backup invokes the **savepnp** program instead of the **save** program. The first time the client is backed up, **savepnp** creates a default backup program file, which you can then customize for future backups of the client.

Additional processing instructions can be specified by entering the name of a custom script in the Backup Command attribute in the Client resource. The script is run instead of the default **save** program, when scheduled backups are initiated. The instructions in the script run separately for each **save** set backed up for the client.

When you use the **save** program, a new instance of the customized script is invoked for each **save** set listed in the client’s **Save Set** attribute, rather than just once for that client (as happens with **savepnp**). If you specify a **save set** value of All, the program is run for each file system on the client. As a result, if you create a Client resource with a customized backup for a database, a command to shut down the database is run for each **save** set that is listed.

#### **NOTICE**

After the creation of a customized backup script for a client, try backing up the client immediately. Any configuration or network problems that could prevent a backup should become apparent during this test.

---

The syntax used in the backup script or batch file must adhere to these criteria:

- The program name must begin with either the prefix save or nsr and must not exceed 64 characters.
- The program must reside on the client in the same directory as the NetWorker save command.
- Always specify the full path of the save command in the script.
- The NetWorker save command must be used in the backup program to ensure that the data is properly backed up.
- All commands within the program file must complete successfully. Otherwise, the NetWorker server cannot complete the remaining instructions.
- On UNIX and Linux, when you invoke the NetWorker save command, invoke the command with these arguments: save “\$@”. Doing so enables the save command in the script to accept the arguments usually passed to it by the NetWorker savefs program during a routine backup operation.

## Creating a custom backup script

You can create a custom backup script by using the save program.

### Procedure

1. Use a text editor to create a script in the directory where the NetWorker **save** command resides.

**NOTICE**

For custom backup scripts that are to run on Windows clients, the script name must start with save or nsr and must end with the .bat extension.

Commands in this script must be placed in this order:

- a. Run a preprocessing command before each save set backup (optional).
- b. Back up the data by using the NetWorker **save** command (mandatory).
- c. Run a postprocessing command after each save set backup (optional).
2. In the **Backup Command** attribute of the **Client resource**, type the name of the backup script.
3. Back up the client to ensure that the newly created backup command works.

## Example 1: The save backup command on Windows

In this example, for each save set, the customized backup program runs pre-backup commands, runs the NetWorker save command, and then runs post-backup commands.

The backup program consists of these parts:

- Pre-Backup Command: Redirects the output of the Net start DOS command to create a netstart.txt file at the root of the C: drive and send all current computer Services Started information to this file.
- Save: Runs NetWorker commands required to start the backup process.
- Post-Backup Command: Redirects the output of the Set DOS command to a set.txt file at the root of the C: drive and send all computer system environment information to this file.

The netstart.txt and set.txt files are placed in the C:\directory. New information is appended to these files each time a backup is run.

Also, you can check the batch file execution process in the Monitor Groups tab of the Administration window, or by viewing the savegrp log file in the <NetWorker\_install\_path>\logs directory.

This is an example backup script:

```

@ECHO OFF
SETLOCAL
ECHO ======START BATCH FILE=====
ECHO =====NetWorker PRE_BACKUP COMMAND=====
ECHO =====NET START - creates netstart.txt file and
ECHO =====sends all Started Services information
ECHO =====to the file c:\netstart.txt

NET START >>C:\NETSTART.TXT

REM This command takes incoming arguments from
REM the savegrp command and handle them
REM to overcome batch file limitations:

REM PARSE ALL INCOMING ARGUMENTS
REM and pass single argument in case
REM more than 10 arguments are passed to this file
REM (ie %0-%9 is not enough).

ECHO =====NetWorker SAVE SET COMMAND=====
SHIFT
SET arg=%0

:loop
SHIFT
IF %0==. GOTO save
SET arg=%arg% %0
GOTO loop

REM These are the save commands that run the required
REM NetWorker backup commands.

:save

REM Note: Enter correct path to your NetWorker bin
REM directory (line below is default path)
C:\PROGRA~1\nsr\bin\save.exe %arg%

ECHO =====NetWorker POST_BACKUP COMMAND=====
ECHO ====="SET" - creates set.txt file and sends all
ECHO =====computer system environment information to
ECHO =====C:\set.txt file=====

SET >>C:\SET.TXT

ECHO =====END OF BATCH FILE=====

ENDLOCAL

```

This information is displayed from the Monitor Groups tab, logged to the savegrp.log file after the backup process is done, and verifies the execution of the three processes.

```

--- Successful Save Sets ---
*: jupiter:c:\inetpub ======START BATCH FILE=====
* jupiter:c:\inetpub ===NetWorker PRE_BACKUP COMMAND===
* jupiter:c:\inetpub=====NET START
* creates netstart.txt file and sends all started
* jupiter:c:\inetpub =====services information to
* that file c:\netstart.txt==

* jupiter:c:\inetpub ===NetWorker SAVE SET COMMAND===

```

```

* jupiter:c:\inetpub save: using `C:\Inetpub' for
* `c:\inetpub'
jupiter: c:\inetpub level=full,194 KB 00:00:02 37 files
* jupiter:c:\inetpub =====NetWorker POST_BACKUP COMMAND
* jupiter:c:\inetpub ====="SET" - creates set.txt
* file and sends all computer system
* jupiter:c:\inetpub ===== environment information
* to C:\set.txt file
* jupiter:c:\inetpub =====END OF BATCH FILE=====
jupiter: index:jupiter    level=full, 243 KB 00:00:00      23 files
jupiter: bootstrap           level=full,       47 KB 00:00:00      7
files
* jupiter:bootstrap nsrlpr: Either a printer isn't
* defined for printing the Bootstrap for
* this savegroup,
* jupiter:bootstrap 04/26/06 01:34:13 PM   full
* 3901113601 3901113601 0
jupiter.001

```

## Example 2: The save backup command on UNIX

This script backs up a ClearCase version object base (VOB). The script file must reside in the same directory as the NetWorker save command (for example, on a Solaris system, the save program is installed in the /usr/sbin directory). Type the name of the script into the Backup Command attribute of the Client resource that is used to back up the ClearCase VOB. As a result, this script is invoked instead of the usual save command during a scheduled backup.

**NOTICE**

---

Include the save command in the script and place the script in the same directory as the save program. Otherwise, the backup will fail.

---

This script locks a ClearCase VOB, performs the backup, and then unlocks the VOB.

```

#!/bin/sh
# export the SHELL that we are going to use
SHELL=/bin/sh
export SHELL
# export the correct PATH so that all the required binaries can be
found
case $0 in
/* ) PATH=/usr/atria/bin:/bin:/usr/bin:`/bin dirname $0`\
c=`/bin basename $0`\
;;
* ) PATH=/usr/atria/bin:/bin:/usr/bin:/usr/sbin
c=$0
;;
esac
export PATH

# These are the valid statuses that save reports upon completion of
the backup
statuses="
failed.
abandoned.
succeeded.
completed savetime=
"
# Perform the PRECMD (Lock VOB)
/usr/atria/bin/cleartool setview -exec "/usr/atria/bin/cleartoollock -c \
'VOB backups in progress' -vob /cm_data/mis_dev" magic_view >
/tmp/voblock.log 2>&1

```

```

# Perform backup on client
save "$@" > /tmp/saveout$$ 2>&1
# cat out the save output
cat /tmp/saveout$$
# search for backup status in output reported by save
for i in ${statuses}; do
    result=`grep "${i}" /tmp/saveout$$`
    if [ $? != 0 ]; then
        echo ${result}
    fi
done
# Perform the POSTCMD (Unlock VOB)
/usr/atria/bin/cleartool setview -exec "/usr/atria/bin/
cleartoolunlock -vob
/cm_data/mis_dev" \
magic_view > /tmp/vobunlock.log 2>&
# exit gracefully out of the shell script
exit 0

```

## Controlling the custom backup script exit status reporting

The ability to control the custom backup script is useful for debugging and reporting purposes.

Use the Job Control attribute in the Client resource to control how end of job, and exit status messages are determined for the custom script.

By default, the programs savegrp and nsrjobd determine the success or failure of a custom script based on the completion of the save program (end of job). The following criteria apply:

- If the save job's completion status is success, then savegrp and nsrjobd report that the custom backup job succeeded.
- If the save job's completion status is failure, then savegrp and nsrjobd report that the custom backup job failed.
- If no completion status is received, the custom job's output is examined for completed savetime=savetime lines. If found and the savetime is non 0 (zero), the custom backup job is considered to have succeeded, otherwise it is considered to be failed.
- The exit code of the custom script's process is not taken into consideration.

The Job Control attribute in the Apps and Modules tab of the client resource enables you to change how end-of-job and success or failure messages are determined for a custom script. The Job Control attribute has three options that can be selected singly or in combination. The following table describes these options.

**Table 19** Job Control selections

Job Control selections	Description	Uses
End on job end	A backup job is considered to be ended as soon as an end job message is received from the save command.	Use when you do not want to wait for the post processing commands of the script to end.
End on process exit	A backup job is considered to be ended as soon as the started process exits.	Use when you want your custom script to start background processes and you do not want savegrp or nsrjobd to wait for their completion.

**Table 19** Job Control selections (continued)

Job Control selections	Description	Uses
	Background processes started by the backup command could still be running on the client.	
Use process exit code	Only the process exit code is used to determine the success or failure of the job. An exit code of 0 means success, otherwise the job is reported as failed.	Use when you want the script post processing command status to have an impact on the status of the save backup command without having to unset the NSR_STD_MSG_FD environment variable. If your script invokes more than one NetWorker backup command such as save, you must still unset the NSR_STD_MSG_FD environment variable.
End on job end and End on process exit	Either event can trigger a job's end.	
End on job end and Use process exit code	If an end job message is received before the process exits, then the exit status provided by the end job message is used to determine the job's success or failure.	

## Using the savepnp command with a customized backup program

As an alternative to using the save program with a custom script, use the savepnp command. The savepnp program differs from using a custom script with the save program in that preprocessing and postprocessing commands run only once during the client backup, instead of once for each save set. This command can be useful if the client is running a database or other program that should be stopped before the client is backed up, and then restarted after the backup has completed. The options for the savepnp command are identical to those for the save command.

### Procedure

- From the Administration window, click Configuration.
- In the expanded left pane, select Clients.
- Create a new Client resource or select an existing Client for editing.
- Select the Apps & Modules tab.
- In the Backup Command attribute, type:

**savepnp**

- Back up the client.

The first time a backup group with a client that uses savepnp runs, a standardized group-name.res file is created in one of the following:

- The `/nsr/res` (UNIX)
  - The `NetWorker_install_path\res` (Microsoft Windows) directory on the client
- where group-name is the same as the name in the Group resource selected for that client. If the client belongs to multiple backup groups, a separate group-name.res file is created for each group to which the client belongs.
- The initial group-name.res file contains type, preprocessing, postprocessing, timeout, and abort precmd with group attributes:

```
type: savenpc;
precmd: "echo hello";
pstcmd: "echo bye";
timeout: "12:00pm";
abort precmd with group: No;
```

#### NOTICE

The abort precmd with group attribute determines what will happen to the preprocessing command when the savegroup process aborts prematurely. By default, the preprocessing command process will not be killed if the savegroup process aborts prematurely. To kill the preprocessing command when the savegroup process aborts, set abort precmd with group to Yes.

---

When the group-name.res file exists, use a text editor to customize the file's attributes. These customized instructions are then applied the next time the client is backed up.

Before performing a save operation on the client, the modified savenpc program performs the following:

- Any preprocessing commands listed for the precmd attribute in the group-name.res file.
- The save by using the options specified for the savenpc command itself.
- Any postprocessing commands listed for the pstcmd attribute.

When editing a group-name.res file, these points apply:

- The command environment that is opened by the savenpc command to run a customized backup does not automatically inherit the system's default environment. Specifically, environment variables, including PATH, will either not exist or will be set to NULL. The environment must be built as part of the preprocessing (precmd) commands, especially the PATH variable. On UNIX clients, be sure to source the .profile, .cshrc, and other login scripts.
- The save command should not be specified in the group-name.res file. The savenpc program will automatically invoke the save command and back up the save sets specified in the Save set attribute for the client.
- To exclude the environment variables in the group-name.res file, include full pathnames for all commands and files.
- Resident commands, for which there is no executable file present, like time and dir, will not work as commands in your group-name.res file. The log reports that the executable file could not be found.
- On a Microsoft Windows client, do not use "@ECHO OFF" in the group-name.res file.
- To add more than one command sequence to the precmd and pstcmd attributes, insert a comma (,) to separate the commands.

- A complete command-line for an attribute must end with a semicolon (;).
- Escape any backslash (\) characters in the group-name.res file. For example, the pathname C:\mydir\myprogram.exe must be written C:\\mydir\\myprogram.exe. This is an example of a fully functional group-name.res file:

```
type: savepnp;
precmd: "V:\\usr\\sap\\PDB\\SYS\\exe\\run\\PDB-stop.cmd >
C:\\WINNT\\system32\\PDBStop.log 2>&1";
pstcmd: "V:\\usr\\sap\\PDB\\SYS\\exe\\run\\PDB-start.cmd
C:\\WINNT\\system32\\PDBStart.log 2>&1";
timeout: "12:00pm";
```

It is not necessary to escape any backslash characters in scripts called from the group-name.res. To simplify the pathname issue, include all commands in a script or batch file, and then include that script's full pathname on the precmd or postcmd line.

- A line break is required after the semicolon that ends the last command in the group-name.res file.
- The following applies to text written to standard output:
  - Text written during preprocessing appears in the NetWorker completion notices. You can direct this output to a log file.
  - Text written during postprocessing is discarded. Consider redirecting this output to a log file so you can troubleshoot problems.

The *EMC NetWorker Command Reference Guide* or the UNIX man pages provides information about the `savepnp` command.

## Timeout attribute

The Timeout attribute indicates when the postprocessing commands are to be run, regardless of whether all of the save sets have been backed up or not. The timeout entry must be specified in nsr\_getdate format and must be enclosed in double quotes.

More information on nsr\_getdate is available in the *EMC NetWorker Command Reference Guide* or the UNIX man pages.

If an invalid time is entered for the timeout, the timeout is not reached and an error message is not produced.

The Timeout attribute is optional. To disable the Timeout attribute, add a comment character (#) to the beginning of the line, for example:

```
# timeout: "12:00pm";
```

The value of the Timeout attribute may not be the exact time that postprocessing actually commences. The `savepnp` program's `psclntsav` subroutine uses a one-minute polling interval to check for the completion of preprocessing tasks. Therefore, the `savepnp` log file may show that postprocessing was started up to 60 seconds after the designated timeout.

## Customizing the `savepnp` command for multiple groups

You can customize pre- and postcommand processing for multiple groups.

### Procedure

1. Copy existing group-name.res files.
  - Microsoft Windows clients:

```
NetWorker_install_path\temp\group-name.res to  
NetWorker_install_path\res\ your_new_group.res
```

- UNIX clients:

```
/nsr/res/group-name.res to /nsr/res/your_new_group.res
```

## 2. Edit the new new\_group-name.res file.

If you do not have an existing group-name.res file, activate the group for savenpc without the presence of this file. A default template will be created at one of the following:

- /nsr/res/your\_new\_group.res
- NetWorker\_install\_path\res\your\_new\_group.res

You can then customize the template.

## Message logging by the savenpc command

Messages generated by savenpc are written to the savenpc log file.

The savenpc log file is located in these locations on the NetWorker client:

- UNIX: /nsr/logs
- Microsoft Windows: NetWorker\_install\_path\logs

The format of the savenpc log file is similar to:

- 04/03/07 13:56:43 preIntSave: All command(s) ran successfully.
- 04/03/07 13:57:43 preIntSave: All save sets on the worklist are done.

# Considerations for backing up raw partitions

The NetWorker software must have exclusive access to a file system to perform a raw backup. Close as many applications as possible before doing a raw disk backup. If the raw partition contains data managed by an active database management system (DBMS), ensure that the partition is offline and the database manager is shutdown. For greater flexibility when backing up partitions that contain DBMS data, use a NetWorker Module application.

## Backing up raw partitions on UNIX

Back up raw disk partitions on UNIX by using the rawasm directive.

## Backing up raw partitions on Windows

Back up a raw disk partition on Windows by specifying the raw disk partition in a save set with the save command.

Identify the raw partition as a physical drive or logical drive. For example:

```
save -s NetWorker_server_name \\.\PhysicalDrive0  
save -s NetWorker_server_name \\.\C:
```

## Backing up access control lists

The backup and restore of Access Control Lists (ACL), and extended ACL is fully supported. This support includes Linux, HP-UX, AIX, DEC, SOLARIS, OS/X, and Windows.

There is no special attribute or keyword that controls this support. When a file with an associated ACL is backed up, the ACL is backed up along with the file data. When the file is recovered, any associated ACL is also recovered.

Enable ACL passthrough in the Recover section in the NetWorker Server Properties window to recover files with associated ACLs.

## BOOT/BCD Data on Windows backups

In earlier versions of the Windows operating system, the BOOT directory was present in the system drive. In Windows 7, Windows 8, Windows 8.1, Windows Server 2008 R2, Windows Server 2012 and Windows Server 2012 R2, a hidden, unmounted system-reserved partition can be present and the BOOT Configuration Data (BCD) store is on this partition. The BCD store contains the boot configuration parameters and controls the computer's boot environment.

The NetWorker Windows client backs up the system reserved partition and the BCD store only for Windows offline Bare Metal Recovery (BMR). During a Windows offline BMR backup, NetWorker checks the type of operating system. If it is Windows 7, Windows 8, Windows 8.1, Windows Server 2008 R2, Windows Server 2012 or Windows Server 2012 R2, NetWorker assigns a GUID to the partition and performs the backup of the BCD. The BCD partition does not need to be mounted for the backup to occur. If the BCD partition is not mounted, the backup is not indexed. The saveset name is GLOBALROOT/xxxxxx/.

The BCD can only be restored as part of a NetWorker Windows offline BMR. Online recovery of the BCD is not available. Consult Microsoft documentation for using the BCDEdit tool to save copies of BCD before making boot configuration data changes.

## Support for backing up renamed directories

As of NetWorker 8.0, the option to back up renamed directories is enabled by default. The Backup renamed directories attribute can be disabled or enabled for each NetWorker client.

Consider the following when deciding whether to disable or enable this feature:

- This feature must be enabled for NetWorker clients that use the synthetic full backup feature.
- When this feature enabled and a renamed directory is encountered, a full backup is performed on all sub-directories and files under a renamed directory.
- When this feature is enabled and if a renamed directory is at some future date given its original name, files and subdirectories under that directory will not be eligible for backup until the files or subdirectories are updated or the next full backup occurs.
- When this feature is disabled, unchanged files and folders under the renamed directory will be skipped during a non-full level backup. This behavior can cause unexpected results during a recovery operation. If you attempt to recover data under a renamed directory from a date between the time that the directory was renamed and the next full level backup, it may appear that data is missing. For that recovery

time period, any files or folders that were unchanged will not display under the renamed directory. Instead, they will be displayed under the old directory name.

## Backing up only client file indexes and the bootstrap

You can set up a backup group to backup only the client file index information for those NetWorker clients that belong to the backup group. The bootstrap will also be backed up.

### Procedure

1. Set up a backup group as described in [Creating groups for backup clients on page 63](#)
2. In the backup group properties Advanced tab, select **Index only** from the **Options** attribute.
3. Click **OK**.

# CHAPTER 3

## Storage Nodes and Libraries

This chapter contains the following topics:

• Storage nodes.....	124
• Storage node configuration.....	124
• Dedicated storage nodes.....	130
• Troubleshooting storage nodes.....	131
• Avamar deduplication nodes and replication nodes.....	131
• Devices and libraries.....	131
• Autodetection of libraries and tape devices.....	132
• Configure libraries.....	134
• Reconfigure libraries.....	136
• Specify available library slots.....	137
• Miscellaneous library operations.....	138
• Tips for using libraries.....	140
• Library maintenance.....	142
• Deleting libraries.....	145
• Troubleshooting autoconfiguration failure.....	145
• Silo libraries.....	146
• Configuring silo libraries.....	147

## Storage nodes

Storage nodes (including the NetWorker server) are host computers with attached storage devices. A storage node has the physical connection and ownership of the attached devices, but the NetWorker server maintains the client file index and media database. With the NetWorker software, client data can be routed directly to a storage node's storage devices without the data first going to the NetWorker server. A storage node may be a client of the NetWorker server, although this is not a requirement. However, the storage node must have the NetWorker client software installed.

From the NetWorker server, typical storage tasks can be performed, such as:

- Mounting and labeling volumes for the storage node devices.
- Configuring NetWorker resources associated with the storage nodes.

Only users who have the Configure NetWorker privilege can add to or change the configuration of the NetWorker server, media devices, and libraries. The EMC NetWorker Security Configuration Guide provides more information.

## Requirements

To operate the NetWorker software with storage nodes, there are requirements that must be met.

- On UNIX systems, this software must be installed on the storage nodes. The packages must be installed in the following order:
  1. NetWorker client software
  2. NetWorker storage node software
  3. (Optional) EMC AlphaStor software.  
This enables multiple NetWorker servers to share the storage node. The AlphaStor software must be used to manage the libraries, drives, and volumes on that node. The AlphaStor server is available on Solaris and Microsoft Windows only. AlphaStor DCP/LCP is available on all UNIX, Linux, and Windows platforms. Refer to the *EMC NetWorker Software Compatibility Guide* for information.
- On Windows systems, the Storage Node Option must be installed. This installs both the NetWorker client and storage node software.

## Licensing

The *EMC NetWorker Licensing Guide* provides information on NetWorker licensing support for storage nodes.

## Storage node configuration

The following sections provide the procedures for configuring a NetWorker storage node.

### Configuring a storage node

The new storage node appears in the navigation tree.

#### Procedure

1. Ensure the storage node software and required enabler codes have been installed on the host.

2. In the NetWorker server **Administration interface**, click the **Devices** view.
3. From the navigation tree, right-click **Storage Nodes** and select **New**.

The Create Storage Node window appears, with the General tab displayed.
4. Set the **Identity** attributes:
  - a. In **Name**, specify the hostname of the NetWorker storage node.
  - b. In **Type of Storage Node**, select a type:
    - SCSI
    - NDMP
    - SILO (or SILO with NDMP) The silo robot arm must not be detected by the NDMP storage node.
5. In the **Status** attributes, review or set the storage node status:
  - a. **Storage node is configured** indicates whether a device has already been configured on this storage node.
  - b. **Enabled** indicates whether the storage node is available for use:
    - Yes indicates available state.
    - No indicates service or disabled state. New device operations cannot begin and existing device operations may be cancelled.
  - c. **Ready** indicates whether the storage node is ready to accept device operations.
6. Set the **Device Management** attributes:
  - a. In **Max active devices**, set the maximum number of devices that NetWorker may use from this storage node in a DDS environment.
  - b. In **AFTD allowed directories**, for AFTD devices, type the pathnames of directories on the storage host where AFTDs are allowed to be created.
  - c. In **mmds for disabled devices**, select a nsrmmmd (data mover) option (see note):
    - Yes to start nsrmmmd processes for disabled devices.
    - No to *not* start nsrmmmd processes for disabled devices.
  - d. In **Dynamic nsrmmds**, for AFTD or DD Boost devices, select whether nsrmmmd processes on the storage node devices are started dynamically.
    - Selected (dynamic mode): NetWorker starts one nsrmmmd process per device and adds more *only* on demand, for example, when a device Target Sessions is reached.
    - Unselected (static mode): NetWorker runs all available nsrmmmd processes. In environments where unattended firewall ports need to be restricted for security reasons, the storage node settings for mmds for disabled devices and Dynamic nsrmmds *unselected* (static mode) offer more control because they cause all available nsrmmmd firewall ports to be attended by running nsrmmmd processes.
7. In **Remote Host**, if an NDMP tape library is used by this storage node, type the **Remote User name** and **Password**. Only one user is allowed per storage node.
8. Select the **Configuration** tab.
9. In **Scanning**, set the attributes for SCSI library target devices on this storage node:
  - a. In **Device Sharing Mode**, select an option:

- Server Default uses the NetWorker server setting for device sharing.
  - Maximal Sharing allows sharing of all devices.
  - No Sharing disables device sharing.
- b. In **Search all LUNs**, select an option:
- Yes for NetWorker to detect all LUNs (logical unit numbers). Detection can take a long time.
  - No (default) for NetWorker to stop searching at the first available LUN.
- c. In **Use persistent names**, choose whether NetWorker uses persistent device names specific to the storage host operating system when performing device discovery and autoconfiguration operations.
- d. In **Skip SCSI targets**, list any SCSI targets to exclude from backup operations, one per line, if the storage node type is set to SCSI. The format is bus.target.lun where the target and LUN fields are optional. You can exclude a maximum of 63 targets.
10. In **Advanced Devices**, for AFTD or DD Boost devices, configure the settings:
- In **Server network interface**, type the unique network interface hostname of the NetWorker server to be used by the storage nodes.
  - In **Clone storage nodes**, list by priority the hostnames of the storage nodes to be used for the save or “write source” side of clone operations originating from this storage node as the “read source.” The clone operation selects the first storage node in this list that has an enabled device and a functional nsrmmmd process. If this attribute has no value, then the NetWorker server’s storage node Clone storage nodes attribute is used, and if that has no value then the NetWorker client’s Storage nodes attribute is used.
- In backup-to-disk environments it is possible for a single backup volume to be shared by multiple storage devices on different storage nodes. This can result in an ambiguous clone write source.

11. When finished, click **OK**.

## Modifying the timeout attribute for storage node operations

An attribute named Nsrmmmd Control Timeout, which is set during NetWorker server configuration, configures the amount of time a NetWorker server waits for a storage node request to be completed. If the timeout value is reached without completion of the request, the operation stops and an error message is logged. The default value assigned to Nsrmmmd Control Timeout is five minutes.

### Procedure

1. In the server’s **Administration interface**, click the **Configuration** button.
2. Select **View > Diagnostic Node**.
3. Right-click the NetWorker server in the left pane and select **Properties**.
4. Select the **Media** tab.
5. Modify the attributes as appropriate and click **OK**.

## Configuring timeouts for storage node remote devices

Timeouts that determine how long to wait for mount requests on a storage node remote device before the save is redirected to another storage node are set in a device's Properties.

The Storage Node Devices area of the tab includes these attributes related to storage node timeouts:

- Save Mount Timeout
- Save Lockout

Save Mount Timeout and Save Lockout attributes to change the timeout of a save mount request on a remote device.

If the mount request is not satisfied within the time frame specified by the Save Mount Timeout attribute, the storage node is locked out from receiving saved data for the time specified by the Save Lockout attribute.

The default value for Save Mount Timeout is 30 minutes. The default value for Save Lockout is zero, which means the device in the storage node continues to receive mount requests for the saved data.

### Note

The Save Mount Timeout applies only to the initial volume of a save request.

To modify these attributes:

### Procedure

1. In the server's **Administration interface**, click the **Devices** button.
2. Select **View > Diagnostic Node**.
3. Right-click the remote device and select **Properties**.
4. Select the **Advanced** tab.
5. Modify the attributes as appropriate and click **OK**.

## Configuring the client's storage node affinity list

The choice of which NetWorker servers and storage nodes receive a client's data—known as *storage node affinity*—is made by entering their hostnames in the Storage Nodes attribute located in the Client Properties, on the Globals (2 of 2) tab. The default setting for the Storage Nodes attribute on most Client resources is nsrserverhost (the host NetWorker server).

If the Client resource of a storage node computer is created after a remote device on the storage node has been created, the default setting of the Storage Nodes attribute is the storage node and the NetWorker server.

If you create a Client resource after you create a storage node, and you will configure the client to back up to that storage node, enter the name of the storage node in the Storage Nodes attribute of the Client resource above the default nsrserverhost. You can add Storage node names to the Storage Nodes attribute list at any time. The NetWorker software directs the client data to the first storage node in the list with an enabled device, capable of receiving the data. The NetWorker software sends additional saves to the next storage node in the Storage node list based on the criteria specified in [Balancing the load on the storage node on page 128](#).

To modify the Storage Nodes attribute:

### Procedure

1. In the server's **Administration interface**, click the **Configuration** button.
2. Select **Clients**, right-click the appropriate client and select **Properties**.
3. Select the **Globals (2 of 2)** tab.
4. Modify the **Storage Nodes** attribute as appropriate and click **OK**.

## Balancing the load on the storage node

Starting in NetWorker 8.1, a new feature, named Save session distribution, has been introduced that allows one to configure how save sessions are distributed among storage nodes.

---

### Note

This feature is not available for clone and recover operations.

---

The Save session distribution feature can be applied to all NetWorker clients globally or to selected clients only. This feature has two options:

#### **max sessions**

Save sessions are distributed based on each storage node device's max sessions attribute. This is the default distribution method.

#### **target sessions**

Save sessions are distributed based on each storage node device's target sessions attribute. This option is more likely to spread the backup load across multiple storage nodes, while the max sessions option is more likely to concentrate the backup load on fewer storage nodes.

When the max sessions option is selected, NetWorker client save sessions are distributed among eligible storage nodes as follows:

### Procedure

1. Identify the available storage nodes in the NetWorker client's Storage node affinity list.
2. Use an available device on the first storage node in the list that is working below its target sessions level.
3. When all devices on the first storage node are running at their target sessions level but some are running below their max sessions level, then use the least loaded device.
4. When all devices on the first storage node are running at their max sessions level, continue to the next storage node and repeat the device selection process described previously in steps 2 and 3.
5. Continue until all available devices on all storage nodes in the client's storage node affinity list are in use.
1. When the target sessions attribute is selected, NetWorker client save sessions are distributed among eligible storage nodes as follows:
6. Identify the available storage nodes in the NetWorker client's Storage node affinity list.
7. Use an available device on the first storage node in the list that is working below its target sessions level.

8. When all devices on the first storage node are running at their target sessions levels, continue to the next storage node even if some devices are running below their max sessions level.
9. When all devices on all eligible storage nodes are running at their target sessions level, use the least loaded device that is running below its max session value.
10. Continue with step 4 until all devices on all available storage nodes are running at their max session levels.

## Specifying storage node load balancing

By default, NetWorker balances client backups across storage nodes based on the max sessions attribute for each device on the storage node. If you choose to balance storage node loads by max sessions, you can override this setting for selected clients.

### Procedure

1. In the server's **Administration interface**, click the **Configuration** button.
2. Select **View > Diagnostic Node**.
3. Right-click the NetWorker server in the left pane and select **Properties**.
4. Select the **Setup** tab.
5. Select a value from the **Save session distribution** list.

If you select target sessions, then all NetWorker clients will have their backups balanced across storage nodes based on device target session values. The Save session distribution attribute on each NetWorker client resource is ignored.

If you select max sessions, then you can still override this value for selected NetWorker client resources by setting the Save session distribution attribute in the client resource.

6. Click **OK**.

## Overriding the save session distribution method for selected clients

If you selected max sessions as the Save session distribution method for the NetWorker server, you can override this setting for selected clients.

### Procedure

1. In the server's **Administration interface**, click the **Configuration** button.
2. Select **Clients**.
3. Right-click the appropriate client and select **Properties**.
4. Select the **Globals (1 of 2)** tab.
5. Modify the **Storage Nodes** attribute as appropriate and click **OK**.
6. Select **target sessions** from the **Save session distribution** list.
7. Click **OK**.

## Performance considerations for storage node load balancing

Be aware of the following performance considerations for storage node load balancing:

- Depending on how your backup environment is configured, there is a potential to shorten backup times by using the device target session option rather than the device maximum session option. However, using the device target sessions option with the Checkpoint restart feature can result in slower recovery times because a single save set is more likely to be spread across multiple storage nodes.

- Each NetWorker client has a storage node affinity list. The Save sessions distribution feature can only distribute a NetWorker client's backup sessions to multiple Storage nodes if the client has two or more storage nodes in its storage node affinity list. The storage node affinity list is specified on the Globals (2 of 2) tab in the NetWorker Client Properties window.

## Bootstrap backup on a storage node

When the server's bootstrap save set is backed up, the data writes to a device that is local to the NetWorker server. A bootstrap cannot be backed up to a remote device, but a bootstrap can be cloned or staged to a remote device. When the `mmrecov` command is used to recover a bootstrap save set, the data must be recovered from a local device.

### Staged bootstrap backups

Bootstrap backups can be directed to a disk device such as an AFTD or FTD device. However, if a bootstrap backup is staged to another device, the staging operation completes and is reported as complete even though the "recover space" operation is not executed. This means that the staged bootstrap remains on the original disk from which it was staged. Therefore, the original disk can be used to scan in the bootstrap data if the staged bootstrap is accidentally deleted. Also be aware that if the bootstrap data is not staged from the original disk, the data on the original disk is subject to the same browse and retention policies as any other save set backup and is subject to deletion after the retention policy expires.

This bootstrap information also applies to NDMP devices.

## Dedicated storage nodes

All devices created on storage nodes (except servers) include the Dedicated Storage Node attribute. A dedicated storage node can back up only its own, local data.

Set this attribute when a device is created on a remote storage node. It is found in the Storage Node Properties, on the Configuration tab. If the Dedicated Storage Node attribute is set to Yes, a Dedicated Storage Node License is required for the storage node. If, however, the Dedicated Storage Node attribute is set to No (the default value), a standard storage node license is required. The Dedicated Storage Node License also can be used for backing up virtual clients in a cluster.

### NOTICE

A storage node host cannot mix storage node types. Either all devices on a storage node must be set up for a dedicated storage node, or all must be set up for a standard storage node.

NetWorker supports the installation of a dedicated storage node in a Solaris 10 local zone to backup directly to a physically attached device without sending data across the IP network. NetWorker allows sharing of a device between multiple dedicated storage nodes that are installed in multiple local zones of a single physical host, assuming all the storage nodes belong to a single NetWorker data zone.

## Troubleshooting storage nodes

If a backup fails, this message might appear:

```
no matching devices; check storage nodes, devices or pools
```

The problem could be related to storage node affinity.

Possible causes include:

- No enabled devices are on the storage nodes.
- The devices do not have volumes that match the pool required by the backup request.
- All devices are set to read-only or are disabled.

For example, if the client has only one storage node in its Storage Node list, and all devices on that storage node are disabled, fix the problem and then restart the backup.

Complete one of the following actions to fix the problem:

- Enable devices on one of the storage nodes in the client's list.
- Correct the pool restrictions for the devices in the storage node list.
- Configure an additional storage node that has enabled devices that meet the pool restrictions.
- Set one of the devices to read/write.

## Avamar deduplication nodes and replication nodes

Deduplication nodes and replication nodes exist on Avamar servers. Contact EMC Customer Support to configure these nodes on the Avamar server side. Once that has been done, you can create access to them from the NetWorker side.

The *EMC NetWorker Avamar Integration Guide* provides information on how to create a NetWorker deduplication node.

## Devices and libraries

NetWorker software supports many different types of tape libraries, also called autochangers or jukeboxes. The general categories of libraries are SCSI, NDMP, and silo.

### SCSI libraries

SCSI libraries have automated robotic mechanisms to move tape media from a fixed number of library slots to devices for read or write operations. The number of slots can typically vary between 2 to 10,000 and the number of devices can be between 1 to 100 or more.

Traditionally, libraries are physical units with mechanical robotics, however the same functionality can also be provided by virtual tape libraries (VTLs) that emulate this functionality. VTLs can also be configured and used as Autochangers.

In all cases, the robotic controller and associated tape devices are all controlled through a SCSI interface which is available on one or more storage hosts.

## NDMP libraries

NDMP libraries or devices are accessed by using the NDMP protocol and are typically used by network attached storage (NAS) systems. These devices do not allow direct access to control from the host operating system. Control and data movement is performed over the network by using the NDMP protocol.

## Silo libraries

Silos libraries have a robotic controller that moves tape media between slots and devices. However silos do not use a SCSI interface to access and control the media movements. The movements are controlled by a separate host that receives requests over the network.

# Autodetection of libraries and tape devices

Autodetection is a scanning process that applies only to physical tape libraries and virtual tape libraries (VTLs). The NetWorker software automatically discovers libraries and devices that are being used for backups and recoveries.

The maximum number of configured devices for any NetWorker server and storage node combination is 512. The maximum number, including non-configured devices, can vary depending on the specific server that is being administered.

The following options are available from many of the menus throughout the Devices task:

- Configure all Libraries
- Scan for Devices

If you start these options from the server folder instead of from the storage node folder, then all storage nodes on the NetWorker server are automatically selected for configuration in the wizard, or for scanning, respectively.

As with other Console functions, you can view and work with only those NetWorker servers for which you have access permission.

### NOTICE

Autodetection should not be used for devices on a Storage Area Network (SAN) while any of the devices are in use, because this may cause the device in use to become unresponsive. To avoid this situation, do not configure a device in multiple NetWorker datazones.

## Scanning for libraries and devices

Devices already known to the NetWorker server can be seen in the enterprise hierarchy in the navigation tree. Use the Scan for Devices option described here to find devices that are not yet known to the NetWorker server. Be aware that:

- A storage node must be added to the hierarchy before its devices can be scanned.
- The Scan for Devices option does not detect file type or advanced file type devices.
- By default, the Linux kernel configures a maximum of 128 st devices by default. Refer to [The inquire command and the Scan for Devices operation do not detect more than 128 tape devices on page 727](#) if the Scan for Devices option does not detect more than 128 tape devices on Linux operating systems.

- A specific network interface can be used between the NetWorker server and the storage node when scanning for devices. [Identifying a specific network interface for device scan operations on page 133](#) provides more information.

### Procedure

1. In the **Console** window, click **Enterprise**.
2. In the navigation tree, select a NetWorker server.
3. In the **Name** column of the **Host detail** table, double-click **NetWorker**. The **NetWorker Administration** window for the selected server opens. Note that while multiple **NetWorker Administration** windows can be open simultaneously, each one displays information about only one host or server.
4. In the **Administration** window, click **Devices**.
5. In the navigation tree:
  - a. Right-click the server name, and select **Scan for Devices**.
  - b. Click the storage node to be scanned.
  - c. If the appropriate storage node is not listed, click **Create a New Storage Node**.
  - d. When creating a new storage node, replace the default value in the **Name** field with the fully-qualified domain name or short name of the new storage node.
  - e. Fill in any required information, such as whether to scan for SCSI or NDMP devices and whether to search all LUNs.
  - f. Click **Start Scan**. To monitor the scan activity, click **Monitoring**, then select the **Log** tab. Any relevant status information is displayed there.
6. Return to the **Devices** navigation tree to view the refreshed device information (configured and unconfigured):
  - To display SCSI and NDMP libraries available to the NetWorker server, select **Libraries** in the navigation tree. Any available library or silo appears in the **Libraries detail** table.
  - To display stand-alone devices available to the NetWorker server, select **Devices** in the navigation tree. Any available stand-alone device appears in the **Devices detail** table, along with devices available in libraries.
  - To display the libraries and devices that are available to a storage node, select the storage node in the navigation tree. Available storage nodes appear in the table. Double-click a storage node to see its details, along with the devices that are available in the storage node.

### Identifying a specific network interface for device scan operations

If the NetWorker server has multiple network interfaces, you can specify that a specific network interface be used for scan operations. In this case, the dvdetect (device scan) program will use the specified network address or hostname to communicate with the NetWorker server.

### Procedure

1. In the server's **Administration interface**, click the **Devices** button.
2. Select **View > Diagnostic Mode**.
3. In the left pane, click on the **Storage Nodes** folder.
4. In the right pane, select a storage node.
5. Right-click the storage node and select **Properties**.

6. Select the **Configuration** tab.
7. In the **Server network interface** field, type the network address or the unique hostname of the network interface on the NetWorker server that is to be used.
8. Click **OK**.

## Refreshing enterprise library views on request

### Procedure

1. From the **Console** window, click **Libraries**.
2. In the navigation pane, select a server to update, or select the top item in the hierarchy to update library information for all NetWorker servers.
3. Right-click the server, and select **Refresh**.

## Changing the polling interval for enterprise library views

Enterprise library views are updated periodically without user intervention.

### Procedure

1. From the **Console** window, click **Setup**.
2. From the **Setup** menu, select **System Options**.
3. In the **Polling Interval for NetWorker Libraries** field, type the appropriate time, in hours.
4. Click **OK**.

## Configure libraries

A library resource must be created for each library, including silos, on a storage node. Because a NetWorker server is also a storage node, this procedure applies to a NetWorker server and all of its storage nodes. You can configure a library either automatically with the configure all libraries wizard or manually with the user interface.

A storage node must be created before devices can be configured to be used by them. [Storage nodes on page 124](#) provides details. All scanning for devices is performed at the storage node level and can be performed across multiple storage nodes.

Only devices that have serial numbers can be autoconfigured. Use the `jbconfig` command to configure devices that do not have serial numbers (the `inquire` or `sn` commands can be used to determine if a device returns a serial number).

Devices must be updated to the most recent firmware and drivers.

The following library types can be automatically configured:

- SCSI
- NDMP
- Silo (except DAS silo)

The following device types must be configured by using the `jbconfig` command:

- AlphaStor devices.
- IBM tape libraries controlled through the use of IBM's tape driver. (This is because the device autodetection code uses the internal `lus` driver to control libraries.)
- Any library that does not return a serial number for the robotic arm or any of its tape devices.

## Adding a library resource

### Procedure

1. In the server's **Administration** interface, click **Devices**.
2. Open the **Storage Nodes** folder in the navigation tree.
3. Right-click the storage node to which the device is to be configured, and select **Configure All Libraries** (which is available from many of the menus throughout the **Devices** task). This opens a wizard that can configure all detected libraries, except those explicitly excluded in the library exclusion list during configuration.

**NOTICE**

If **Configure All Libraries** is started from the server folder instead of from the **Storage Node** folder, then all storage nodes on the NetWorker server are automatically selected for configuration in the wizard.

The **Configure All Libraries** wizard appears. This lets you step through library configuration, including this input (some of which is filled in by default):

- Library type (select **SCSI/NDMP**).
  - An NDMP remote username and a password are required for an NDMP device that acts as a storage node.
  - Adjust the **Enable New Device** option, if necessary.
  - Current server sharing policy. Use maximal sharing with Dynamic Drive Sharing (DDS). By default, the sharing policy is displayed as "server default," which is maximal sharing.
  - Storage nodes to which libraries can be configured (select a storage node to see its details). If the appropriate storage node is not listed, click **Create a New Storage Node**.
  - When creating a new storage node, replace the default value in the **Name** field with the fully-qualified domain name or short name of the new storage node.
  - Update storage node properties, if required.
4. After specifying the required information, click **Start Configuration**. The configuration window displays a message that the **Configure All Libraries** process has started. The status of the configuration activity can be viewed by the **Monitoring > Log** screen.
  5. When the configuration is complete, click **Finish** to close the configuration wizard. If problems occur during configuration, you can click the **Back** button on the configuration window to adjust the settings.

## Virtual tape library (VTL) configuration

During library configuration, the NetWorker software automatically attempts to detect if a library is a VTL, and updates the read-only Virtual Jukebox attribute to Yes, or if not, to No. VTLs that are mistakenly identified as autochangers can indicate what type of license should be used, either autochanger or VTL.

### VTL licensing

The *EMC NetWorker Licensing Guide* provides information about NetWorker licensing support for a Virtual Tape Library.

## Queuing device resources for AlphaStor

Because the NetWorker software detects devices as virtual devices, users can request more devices than actually exist. The AlphaStor software queues these requests, and can prioritize them according to whether a tape is mounted for reading, or for writing. This allows AlphaStor users to prioritize recovery operations above backups or other operations that might compete for the same devices.

This feature requires AlphaStor release 3.1 or later.

Configure the AlphaStor library by using the `jbcfg` command.

For information about configuring resource queuing, refer to the *EMC AlphaStor Administration and Operator's Guide*. The `nsr_mount_request` man page describes the resource-queuing feature. Related attributes are also in the `nsr_pool` and `nsr_jbox` UNIX man pages and the *EMC NetWorker Command Reference Guide*.

## Reconfigure libraries

Configure NetWorker privilege is required to reconfigure a library or to add or remove access paths to the devices in a library. This includes access paths that allow libraries to be shared.

Considerations when reconfiguring a library:

- The reconfiguration of stand-alone or file type devices is not supported. Instead, delete the stand-alone or file type device, and then create a new one.
- The following procedure does not support adding NDMP devices to a non-NDMP library if both the NDMP server and the NetWorker storage node are on the same host. Instead, use the `jbedit` command.

## Reconfiguring a library

### Procedure

1. Run **Scan for Devices**, in case a device path has been added to, or removed from, the library since the latest scan.
2. In the server's **Administration** window, click **Devices**.
3. Select **Libraries** in the navigation tree. The **Libraries detail** table appears.
4. In the navigation tree, right-click the entry for the library to be reconfigured, or open the **Storage Nodes** folder, open the library folder, and then right-click the library entry there.
5. Select **Reconfigure Library**. The **Reconfigure Library** window appears. Note that the storage node name and library name cannot be changed in this window.
6. Make appropriate changes in the **Configure devices on various storage nodes using existing drive connectivity** area, selecting or clearing checkboxes as necessary, or using the buttons at the right side of the area (**Check All**, **Clear All**, **Reset**).

Drives that are already configured to be used by the library display check marks in the boxes adjacent to their names:

- Selecting a box adds the drive to the library.
- Clearing a box removes the drive from the library.
- The **Reset** button returns the checkboxes to the condition they had when the Reconfigure Library window was opened.

7. Click **Start Configuration** to reconfigure, or **Cancel** to leave the window.
8. Run **Scan for Devices** to refresh the navigation tree and show the reconfiguration results.

## Library configuration using the jbedit command

The jbedit (jukebox edit) program can be used as a fallback means of editing library configurations if the autoconfiguration program cannot be used. This command can be run on a NetWorker server, storage node, or client (if the client is a storage node). It operates without disrupting any backup or recovery operations on the library.

Running the jbedit program requires Configure NetWorker privileges.

The jbedit program supports all direct-attached SCSI/SJII, SAN, and NDMP libraries. It does not currently support AlphaStor libraries.

The jbedit program is not intended to be a full-fledged editor of the Library resource. The editing of Library resource attributes should be done as described in [Reconfigure libraries on page 136](#). The jbedit options provide selection lists that make it easy to find drives or devices to be added or deleted.

The following table lists the most commonly used jbedit program options.

**Table 20** Common jbedit options

Option	Description
-a	Add a drive or device.
-d	Deletes a drive or device.
-j	Name of the autochanger to be edited.
-f	Name of the device to be added or deleted.
-E	Element address of the device to be added or deleted.

The *EMC NetWorker Command Reference Guide* or the UNIX man page provides a detailed description of the jbedit command, its options, and associated diagnostic messages.

## Specify available library slots

The available slots feature controls which volumes the NetWorker server uses for backup. The server uses all of the volumes in a library to perform recoveries, but the volumes that are automatically selected for backups can be controlled by designating a range of available slots in the library.

### Specifying library slots

#### Procedure

1. Ensure that volumes have been placed in all the available slots of the library so that the NetWorker server can proceed uninterrupted with an automatic backup.

With two-sided media, the number of available slots is effectively doubled. For example, with 32 optical disks labeled “jupiter.001.a” to “jupiter.032.b,” there is a total of 64 sides and, therefore, 64 slots from which to choose.

2. In the server’s **NetWorker Administration** interface, select **View > Diagnostic Mode** from the menu bar.

3. Click **Devices**.
4. Open the **Libraries** folder in the navigation tree. The **Libraries** detail table appears.
5. In either the navigation tree or in the Libraries detail table, right-click the library on which the slots are to be designated, and select **Properties**.
6. Select the **Advanced** tab of the **Properties** window.
7. In the **Media Management Area**, in the **Available slots** field, type a range of contiguous slots, then click **+** to add the range of slots.

For example (assuming that no slots have already been configured), to designate slots 1 through 3 as available, then skip a defective slot 4, and designate slots 5 through 7 as available, type this information in the Available Slots field:

  - a. Type **1-3**, then click **+** to add these slots.
  - b. Type **5-7**, then click **+** to add these slots.
  - c. Click **OK**. Slot 4 will be skipped when tapes are loaded.

## Miscellaneous library operations

This section covers various additional library operation topics.

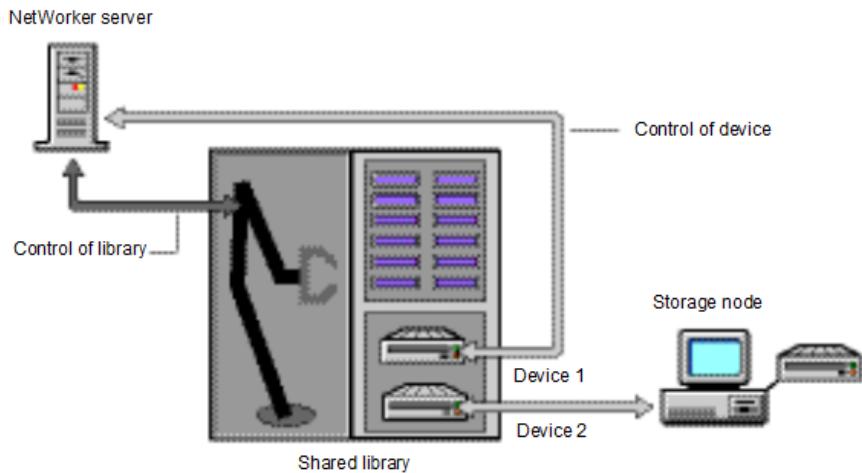
### NetWorker hosts with shared libraries

The NetWorker software permits different NetWorker hosts (a NetWorker server or storage node) within a datazone to control individual devices within a library. This is known as library sharing.

The presence of a SAN within the datazone is not required for library sharing. Dynamic Drive Sharing (DDS) does not support sharing libraries across datazones.

#### How library sharing works

Library sharing enables one NetWorker host to control the library's robotic arm, while other NetWorker hosts (as well as the host controlling the robotic arm) can each control and use specific library devices. A specific device can be controlled only by a single NetWorker host. The following figure shows how multiple NetWorker hosts can share library devices.

**Figure 8** How library sharing works

## Library task inactivity periods

Library resources include attributes used by older, slower libraries that specify the number of seconds a library is inactive after certain operations (such as loading, unloading, or ejecting a volume). For example, once a tape is loaded, the library must read and, possibly, reposition the tape before the next operation can begin. This period of delay is known as *sleeping*.

While sleeping, the library cannot receive or perform other operations. Without the sleep period, the loading or unloading of volumes might fail.

The NetWorker software automatically configures default sleep periods. Change these values only when troubleshooting a library's performance, or if a NetWorker technical support specialist requests it. Typically, the higher the sleep values specified in the attributes, the longer it takes the library to perform the task. Be cautious when changing these values.

The sleep attributes and their default values are shown in this table.

**Table 21** Library resource sleep attributes

Attribute	Description	Default value
Load Sleep	Number of seconds that the NetWorker software waits for a library to complete loading a cartridge.	15 seconds
Unload Sleep	Number of seconds that the NetWorker software waits for a library to complete unloading a cartridge.	60 seconds
Eject Sleep	Number of seconds that the NetWorker software waits for a an eject operation to complete.	60 seconds
Deposit Timeout	Number of seconds for a library to wait for a tape to be deposited in the mail slot before it times out.	15 seconds
Withdraw Timeout	Number of seconds for a library to wait for a tape to be withdrawn from the mail slot before it times out.	15 seconds

**Table 21** Library resource sleep attributes (continued)

Attribute	Description	Default value
Cleaning Delay	Number of seconds that the NetWorker software waits between the completion of a drive cleaning operation and the ejection of the cleaning cartridge from the drive.	60 seconds
Idle Device Timeout	The number of minutes NetWorker will allow a device with a volume to be idle before automatically unmounting it. For specific devices, this value can be overridden. <a href="#">Unmounting volumes automatically (idle device timeout) on page 217</a> provides more information.	10 minutes
Port Polling Period	Number of seconds for a library to wait before polling a mail slot to check for the updated status.	3 seconds

## Server Network Interface attribute

The Server Network Interface attributes in the Device resource are used to determine the network address or the hostname used by the `nsrmmd` program to communicate with the NetWorker server. Similarly, the Server Network Interface attribute in the Library resource is used to determine the network address or the hostname used by the `nsrlcpd` program to communicate with the NetWorker server. These attributes are displayed in the NetWorker Console in diagnostic mode only. The Server Network Interface attributes are only relevant if the device or library is connected to a storage node.

---

### Note

For devices, the `nsrmmd` program will read the Server Network Interface value for the first enabled device from the list of storage node devices, and each subsequent `nsrmmd` started by the NetWorker server will use the same value. Therefore, the NetWorker server will always use the same Server Network Interface value for every `nsrmmd` it starts or restarts, regardless of whether or not the Server Network Interface attribute is different for each device.

---

## Tips for using libraries

This section provides additional suggestions for using libraries effectively and reliably.

## Library notifications

The NetWorker server uses notifications to send messages about NetWorker events. Several preconfigured notifications, such as the following, provide information about various situations:

- Volumes in the library are 90% full
- Library needs more volumes to continue
- Library has a mechanical problem
- Library device needs cleaning
- Cleaning cartridge needs attention.

The NetWorker software automatically mounts a required volume as long as the volume is loaded in the library. If a recovery operation requires a volume that is not loaded in the library, the Tape mount request 1 notification sends an alert to Monitoring > Alerts, with a request to do something with a specific volume.

After a library problem is corrected, it might be necessary to mount a volume so the NetWorker server can continue to back up or recover files.

## Reset a library

A library must be reset each time the library and the NetWorker software become out of sync. A library reset can be done using either the Administration interface or the command prompt.

### Resetting a library in the Administration interface

To reset a library in the Administration interface:

#### Procedure

1. In the **Administration** window, click **Devices**.
2. Open the **Libraries** folder in the navigation tree. The **Libraries** detail table appears.
3. Select a library in the navigation tree or double-click a library in the **Libraries** detail table to open the double-panned **Library Operations** view.

The library's drives are listed in the pane on the left in the Device column. The library's slots are listed in the pane on the right.

4. Right-click a library in the **Device** column, and select **Reset**. You are prompted to reset the library.
5. Click **Yes**. The **Library Operation** window appears and displays this message:

```
The library operation has started.  
Please see the Monitoring->Operations screen for its status.
```

6. Click **OK**.

### Resetting a library from the command-prompt

Use the nsrb -HE command to reset a library from the command prompt. For example, the library inventory must be correct after adding drives to an SJI-compliant library, such as adding DLT7000 drives to an ETL 7/3500 device.

To make the NetWorker software aware of these new drives, execute nsrb -HE to reset the library. The -E option reinitializes the library's element status. Some libraries can keep track of whether there is media in a component in the library. This feature is known as an *element status* capability.

A series of commands exists that allow direct interaction with libraries (sji commands) and tape drives (cdi commands). These commands should only be used by the most knowledgeable of NetWorker users, as the consequences of using them can be unknown. For information about these commands, refer to the *EMC NetWorker Command Reference Guide* or the UNIX man pages.

## Pools with libraries

If the backup strategy includes both full and nonfull backups, estimate the number of volumes needed for the full backups and assign them to the Full pool. This ensures that the full backups are located in a consecutive range of slots in the library. This allows all of the volumes to be removed at the same time.

## Adding and removing media by using the library front panel

Certain media libraries allow for media to be added and removed by using the front panel display. This operation circumvents the NetWorker server's normal procedures for adding and removing volumes and may cause the server information to become out of sync with the library. Normally, you should use the NetWorker server procedures for adding and removing media, rather than the library's front panel display. This is more efficient and guarantees that the server and the library will be in sync.

If it is necessary to use the library's front panel display to add and remove volumes.

---

### Note

When a library is partitioned, the NetWorker software does not become aware of the partitioning. This means that the entire physical library will be disabled, not just one partition.

---

### Procedure

1. In the **Properties** window for the Library, on the **General** tab, set **Status Enabled to Service**.

---

### Note

Putting the library in service mode will cancel all operations or wait for operations to complete that cannot be canceled, and then put the library into disabled mode.

2. Once the library is in disabled mode, use the library's front panel to add and remove tapes.
3. In the **Properties** window for the Library, on the **General** tab, set **Status Enabled to Enabled**.
4. Inventory the library. [Inventorying library volumes on page 219](#) has information about inventorying libraries.

## Library maintenance

Periodically clean a storage library to keep it working correctly. The NetWorker server provides automatic cleaning of devices located in libraries. The server does not support automatic cleaning for stand-alone devices. Cleaning is an option set during configuration.

The service mode feature allows a library to be taken offline temporarily for cleaning or other maintenance.

## Automatic tape device cleaning

Tape device cleaning is an automated, self-contained operation. It is no longer part of a media-loading operation. Tape device cleaning is automatically triggered if one of these conditions exist:

- The last time the device was cleaned was a full cleaning interval ago.
- The Cleaning Required attribute for the device is set to Yes in one of the following ways:
  - Manually by the user.
  - Automatically by the NetWorker server, after it receives a “device needs cleaning” notification.

When one of these conditions is met for a device, cleaning begins as soon as the device becomes available. Loaded devices are unloaded before a cleaning operation begins. Loading a cleaning cartridge (with the nsrjb -l cleaning cartridge command) to force a cleaning operation is no longer supported.

## Selecting a tape device manually for cleaning

### NOTICE

Do not enable automated cleaning for silos in the NetWorker software. The automated device cleaning feature cannot be used in a silo, because it depends on fixed slot numbers. For information about how to clean devices in a silo, refer to the silo manufacturer's software documentation.

### Procedure

1. In the server's **NetWorker Administration** interface, click **Devices**.
2. Open the **Libraries** folder in the navigation tree and select the drive that contains the mounted volume with the block size being checked. The drive's detail table appears.
3. Right-click the drive in the detail table, and select **Properties**. The **Properties** window appears.
4. Select the **General** tab.
5. Set the **Cleaning Required** attribute to **Yes**.

## Delaying tape device cleaning

Occasionally it is necessary to set the **Cleaning Delay** attribute in order to allow a tape device to sleep before attempting to unload a cleaning cartridge.

### Procedure

1. In the server's **NetWorker Administration** interface, click **Devices**.
2. Select **View > Diagnostic Mode**.
3. Open the **Libraries** folder in the navigation tree.
4. Right-click the appropriate library in the detail table, and select **Properties**. The **Properties** window appears.
5. Select the **Timers** tab.
6. Select a value in seconds for the **Cleaning Delay** attribute.

## Tape alert

The TapeAlert feature provides, among other things, diagnostic information for devices for which hardware cleaning is enabled. NetWorker provides the following attributes for tape device cleaning:

- Cleaning required
- Cleaning interval
- Date last cleaned

When the Common Device Interface (CDI) is enabled, TapeAlert attributes provide tape drive status. SCSI Commands must be selected for the CDI attribute on the Configuration tab of the relevant device's Properties. If CDI cannot be enabled, TapeAlert is not supported.

Devices that are capable of TapeAlert perform constant self-diagnostics and communicate the diagnostic information via the nsrmmdd program to logs that can be viewed in the Monitoring task.

TapeAlert attributes are found in the device's Properties, on the Volume tab. Their respective descriptions are as follows:

- TapeAlert Critical: Displays critical diagnostic information, such as for media or drive failure, when user intervention is urgent and data is at risk.
- TapeAlert Warning: Displays a message when the media or device needs servicing.
- TapeAlert Information: Displays status information.

The following table describes the nature of the tape alert levels.

**Table 22** Tape alert severity

Severity	Urgently requires user intervention	Risks data loss	Explanatory
Critical	X	X	
Warning		X	X
Informative			X

The messages indicate tape and drive states related to tape drive read/write management, cleaning management, or drive hardware errors.

## Informative messages

Informative messages indicate status information:

- A data or cleaning tape is nearing its end of life.
- A tape format that is not supported.

---

### Note

When automatic cleaning is enabled, a diagnostic message to indicate that a drive needs cleaning initiates NetWorker drive cleaning.

---

## Warning messages

Warning messages indicate the following types of drive errors:

- Recoverable read or write errors occurred.
- Media is at end of life.
- Read-only tape format is in the drive.
- Periodic cleaning is required.

## Critical messages

Critical messages are warnings that a drive might be disabled and requires immediate attention to avoid data loss:

- Unrecoverable read or write errors occurred.
- Tape is marked read-only.
- Drive require immediate cleaning.
- Drive is predicting hardware failure.

Informative and warning messages should clear automatically by nsrmmd once the reported issue is handled.

Critical messages about hardware errors are not cleared by nsrmmd because they might indicate intermittent hardware problems.

## Deleting libraries

The library's devices remain, and can still respond to NetWorker operations (such as monitoring, labeling, deletion, and so on) after the library definition is deleted. A deletion of a library deletes the library, not its devices.

### Procedure

1. In the server's **Administration interface**, click **Devices**.
2. Select **Libraries** in the navigation tree. The **Libraries detail** table appears.
3. In either the navigation tree or in the **Libraries detail** table, right-click the entry for the library to be deleted, and select **Delete**.
4. When prompted, click **Yes**.

This message appears:

"Are you sure you want to delete this jukebox? If so, please re-attempt deletion within a minute."

5. Click **OK** to confirm the deletion.

## Troubleshooting autoconfiguration failure

Common symptoms of library autoconfiguration failure include the following:

- The library is not listed in the Libraries folder in the Administration interface.
- The library is listed, but is listed as being unconfigured.

Common causes include:

- Device drivers are not properly installed.
- Autodetection fails to match a detected library with its devices due to:
  - Out-of-date device firmware.
  - Failure of the library to return its devices' serial numbers.
- Autodetection failed to start on the storage nodes.

### Procedure

1. Check **Monitoring > Log** for relevant messages.
2. From the command prompt, type the following command to verify that the library returns the serial numbers of its devices:

`sn -a b.t.l.`

where b.t.l. refers to the bus target LUN of the library. If the bus target LUN is not known, run the inquire command first, to obtain this information.

## Silo libraries

This section describes silos and silo devices. Silos and libraries are managed similarly by NetWorker software.

A silo tape library (STL) is a peripheral that usually contains many storage devices. Silos are controlled by silo management software, which is provided by the silo vendor and installed on a silo server. The silo server cannot be the same computer as the NetWorker server.

The silo can be shared among many applications, systems, and platforms. As with libraries, silos make data and media operations more automatic. Silos can load, change, and manage volumes, and clean the devices automatically.

### NetWorker software interactions with a silo

A NetWorker server acts as a client of the silo management software, which resides on the silo server. The NetWorker server communicates with the silo through the Silo Tape Library Interface (STLI), which must be installed on the NetWorker server that uses the silo.

To access the volumes and devices in a silo, the NetWorker server sends a request to the silo management software, in the form of an STLI call. For example, to mount a volume in a silo device, the NetWorker media service sends a request to the silo management software to mount the volume into a particular device in the silo. The silo server responds to the request and mounts the volume in the requested device.

The silo management software controls many of the operations that NetWorker software controls with a library. For example, the silo management software keeps track of the slot where each silo volume resides, and might control the deposit and withdrawal of volumes, as well as automated cleaning of silo devices.

## Installing a silo

### Procedure

1. Install the silo management software on the silo server.
2. Install the **STLI** on the NetWorker server, if required. For more information, refer to the documentation from the silo vendor.

For example, for a NetWorker server or storage node running Windows to control an STK silo, the libattach program must be installed.

On UNIX systems, do not install the STLI library on the following models, because all the necessary software is installed when the NetWorker software is installed:

- IBM 3494 on Solaris and AIX
  - StorageTek on Solaris, AIX, and HP-UX
3. Ensure that the NetWorker server is properly connected to the media devices in the silo.
  4. Add the silo. [Configuring silo libraries on page 147](#) provides details.

## Naming conventions for silo devices

The silo name of the storage devices is supplied during the configuration process. The silo name is the name that the silo management software uses to refer to the storage

device. Depending on the type of silo, the device name can take several forms. This section describes the naming conventions of the currently supported silos.

## StorageTek

The StorageTek (STK) silo management software uses either a program called ACSLS that runs on a UNIX system, or a program called Library Attach that runs on a Multiple Virtual Storage (MVS) system. These programs name devices according to a coordinate system based on the physical location of the devices in the silo.

For tape drives, the name consists of four digits separated by commas:

- The first digit refers to the automated cartridge system (ACS) with which the drive is associated.
- The second digit refers to the library storage module (LSM) in which the drive is located.
- The third and fourth digits refer to the panel and slot location in which the drive is located.

A typical name for an STK drive is similar to: 1,0,1,0.

Ask the silo administrator for the drive names of the devices that the NetWorker server can use. There is no way to get this information from the NetWorker server. To connect to more than one drive, determine the SCSI IDs for each drive and properly match the IDs to the silo names. If the operating system device names and silo names are accidentally swapped, it is only possible to mount and unmount volumes. Volumes cannot be read or written to after they are mounted. To reconfigure the device names properly, use the Administration program to change the order of the device names in the STL Device Names attribute of the library's Properties.

## IBM 3494

The silo management software for the IBM 3494 names devices with an eight-digit number to identify the 3590 drives in the silo. Use the appropriate utility to obtain the device names, as follows:

- On an AIX system, the NetWorker software obtains the name of the device from the device driver and displays the device name as the default value.
- On a Solaris system, the IBM-supplied `mtlib` command (`mtlib -l library_name -D`) must be used to determine the names of all the devices in the 3494, if the silo name is configured by using the `jbconfig` command from the command-prompt, rather than through the configuration interface. Either ask the silo administrator which device is reserved for the NetWorker software, or test to determine which silo drive name matches with each Solaris device name.

# Configuring silo libraries

## Procedure

1. In the server's **Administration interface**, click **Devices**.
2. Open the **Storage Nodes** folder in the navigation tree.
3. Right-click the storage node to which the device is to be configured, and select **Configure All Libraries** (which is available from many of the menus throughout the Devices task). This opens a wizard that can configure all detected libraries, except those explicitly excluded in the library exclusion list during configuration.

---

**Note**

If **Configure All Libraries** is started from the server folder instead of from the **Storage Node** folder, then all storage nodes on the NetWorker server are automatically selected for configuration in the wizard.

---

The Configure All Libraries wizard appears, and allows the user to step through library configuration, including this input (some of which is filled in by default):

- Library type (select **STL Silo**).
- Adjust the **Enable New Device** option, if necessary.
- Current server sharing policy. (Use maximal sharing with Dynamic Drive Sharing (DDS).)
- Storage nodes on which the libraries should configured. You can select a storage node to see its details displayed; if the appropriate storage node is not listed, click **Create a New Storage Node**.

When creating a new storage node, replace the default value in the Name field with the name of the new storage node:

- a. Update storage node properties if required.
  - b. Enter the **Silo Controller** count, which sets the number of silos to be configured for the selected storage node. The default is 1. If a silo count of greater than one is selected, then a library name and hostname must be entered for each one.
  - c. Enter the **Hostname** of the silo controller.
  - d. Enter the **Type of silo** controller. The default is ACSLS Silo (StorageTek).
  - e. (Optional) Use the **Test Silo Controller Connectivity** button to see whether the connection to a silo controller works. Use it once for each silo. An error message appears if the connection to a given silo fails.
4. Click **Start Configuration** after filling in the requested information. The configuration window displays a message that the Configure All Libraries process has started, and that the configuration activity can be viewed by checking the **Monitoring > Log** screen for status.
  5. Click **Finish** on the **Configuration** window to close the configuration wizard. If problems occur during configuration, then the **Back** button on the **Configuration** window becomes active, which allows the user to return to the input screen to adjust input.

## NetWorker software with ACSLS silos

In this section, the term “ACSLS server” refers to the name of the system that is running any one of StorageTek’s library manager programs.

The ssi program is used indirectly by the nsrjb program to communicate with an ACSLS server. The nsrjb program loads libstlstk, which handles the TCP calls to and from the ssi program. The ssi program then handles all of communication to and from the ACSLS server. Starting with ACSLS version 5.3, it is possible to run either a NetWorker server or storage node on the same host that is running ACSLS.

To configure a library, the ssi and mini\_el programs must be running on the system on which library configuration is performed. The ssi and mini\_el programs are generally run as background processes, and are usually started automatically by the system.

In addition to the ssi and mini\_el programs, a shared library file (usually called libstlstk.xxx where xxx is an operating system-dependent extension) is also required. An appropriate version of this library is installed as part of NetWorker installation.

## ACSLS silos and firewalls

With ssi version 2.0, communication with the ACSLS server on a specified port number is supported, using the -a command line option. This is part of the STK firewall enhancement. The ACSLS version 7 must be running on the ACSLS server to use this functionality.

The UNIX man pages for these commands, or see the *EMC NetWorker Command Reference Guide* provides information on the ssi and mini\_el programs.

## Releasing a silo device

When a silo device is configured for use with a NetWorker server, it is possible to restrict silo access only to the NetWorker server. These restrictions allow increased availability to the silo for those with full access. These restrictions can be lifted by using the Release Device feature.

### Procedure

1. In the **Administration** window, click **Devices**.
2. Open the **Libraries** folder in the navigation tree. The **Libraries** detail table appears.
3. Select a silo in the navigation tree or double-click a silo in the **Libraries** detail table to open the double-paned **Library Operations** view. The silo's drives are listed in the **Device** column. The slots are listed in the **Slot** column.
4. Right-click a silo in the **Slot** column, and select **Release Device**. A window appears and asks whether to release devices.
5. Click **Yes**. The **Library Operation** window appears and displays this message:

The library operation has started.  
Please see the Monitoring->Operations screen for its status.

6. Click **OK**.
7. Repeat all steps for each device to be released.

## Silo device cleaning

Do not enable automated cleaning for silos in the NetWorker software. The automated device cleaning feature depends on fixed slot numbers, so it cannot be used in a silo, which does not have fixed slot numbers. For information about how to clean devices in a silo, refer to the silo manufacturer's software documentation.

## Environment variables for StorageTek silos

Environment variables must be set for StorageTek silos. The following table lists the environment variables to set.

**Table 23** StorageTek environment variables

Silo model	Environment variables
StorageTek	For UNIX systems: <ul style="list-style-type: none"> <li>• CSI_HOSTNAME = <i>name_of_ACCLS_system</i></li> </ul>

**Table 23** StorageTek environment variables

Silo model	Environment variables
	<p>The following commands should also be running on the system and can be included in the NetWorker startup script:</p> <ul style="list-style-type: none"> <li>• &lt;binaries_path&gt;/mini_el &amp;</li> <li>• &lt;binaries_path&gt;/ssi &amp;</li> </ul> <p>For Windows systems:</p> <p>The LibAttach Configurator program is available from StorageTek. It creates an ssi process, and a link is available to start the mini_el process from Start &gt; Programs &gt; LibAttach menu tree.</p> <p>Once installed and configured, it starts on reboot.</p>

## Setting environment variables for UNIX systems

### Procedure

1. Create a Bourne shell script file /nsr/nsrrc on the NetWorker server if it does not already exist.
2. Add the variables in this format:

```
ENV_VAR_NAME = value
export ENV_VAR_NAME
```

3. Stop and start the NetWorker server daemons in order for the environment variables to take effect.

# CHAPTER 4

## Backup to Disk and Cloud

This chapter contains the following topics:

- [Types of disk storage devices](#).....152
- [File type devices](#).....156
- [Advanced file type devices](#).....157
- [Changing the AFTD block size](#).....171
- [DD Boost devices](#).....173
- [Cloud devices](#).....173

## Types of disk storage devices

NetWorker software supports a variety of different backup to disk (B2D) methods. These methods all use disk files that NetWorker creates and manages as storage devices. These devices can reside on a computer's local disk or a network-attached disk.

The disk device types that NetWorker supports are FTD, AFTD, DD Boost, and cloud.

This chapter does not cover disk-based devices that emulate other device types, such as virtual tape libraries (VTLs). [Backup to Disk and Cloud on page 151](#) covers VTL devices.

The *EMC NetWorker Licensing Guide* provides information about NetWorker B2D and DD Boost licensing.

### FTD

A file type device (FTD) is a basic disk device type that has been available for many years. FTDs have limited use and support and this chapter describes them for legacy purposes only.

### AFTD

Advanced file type devices (AFTDs) support concurrent backup and restore operations and require the NetWorker DiskBackup Option (DBO) license. AFTDs are supported for the following configurations:

- A local disk on a NetWorker storage node.
- A network-attached disk device that is NFS-mountable to a NetWorker storage node running a Linux or UNIX operating system.
- A network-attached disk device that is CIFS-mountable to a NetWorker storage node running on Microsoft Windows.

The Client Direct feature enables NetWorker clients to back up directly to AFTDs over a CIFS or NFS network, bypassing the storage node. For Client Direct backups, the storage node manages the devices but does not handle the backup data unless the Client Direct workflow is not available.

### DD Boost devices

DD Boost devices reside on Data Domain storage systems that have the DD Boost features enabled. These devices are similar to AFTDs except they store backup data in a highly compressed and deduplicated format. The DD Boost API accesses the DD Boost devices over a network. NetWorker can perform DD Boost backups through either the NetWorker storage node workflow or the Client Direct file access workflow.

The Client Direct workflow enables NetWorker clients with distributed segment processing (DSP) and network access to deduplicate their own backup data and send the data directly to the DD Boost devices. This method bypasses the storage node and frees up network bandwidth. The storage node manages the devices but does not handle the backup data workflow if the Client Direct workflow is available.

If Client Direct backup is not available, NetWorker automatically routes the backup through the storage node where it is deduplicated and sent to the DD Boost devices for storage. Restore operations work similarly. If Client Direct is not available for a restore, then NetWorker performs a traditional storage node recovery.

This guide does not cover DD Boost operations. The *EMC NetWorker Data Domain Deduplication Devices Integration Guide* provides details on DD Boost devices.

## Cloud

Cloud devices are specific to cloud storage services, such as ATMOS. NetWorker accesses cloud services through a private network.

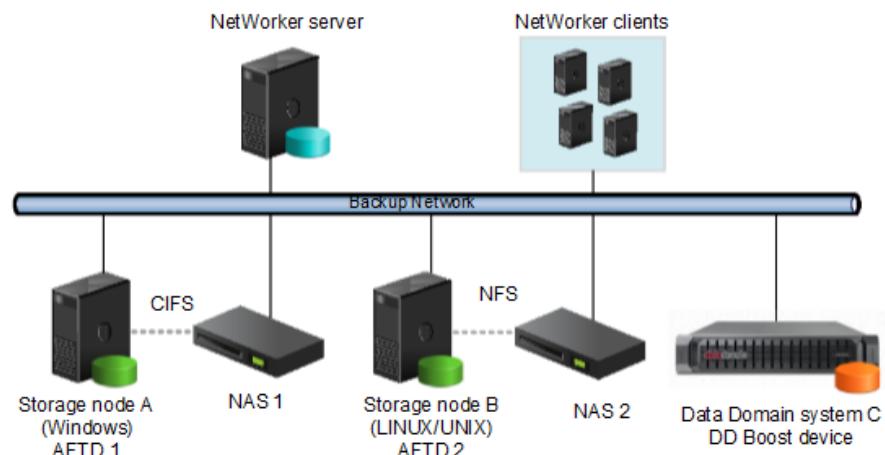
## Example environment

NetWorker backup to disk solutions

The following figure shows various backup to disk options deployed in a mixed operating system environment.

- Linux/UNIX Storage Node A writes its backups to either of the following:
  - The AFTD through an NFS connection to Disk Device 1.
  - The AFTD on Local Disk 1.
- Microsoft Windows Storage Node B uses a CIFS connection to back up to the NAS AFTD on Disk Device 2.
- Data Domain system C writes its backups to a DD Boost device on Local Disk 2.
- 

**Figure 9** Example NetWorker DiskBackup configuration in a mixed backup environment.



## Differences between FTDs, AFTDs, and DD Boost devices

The following table lists the functional differences between traditional file type devices (FTDs), AFTDs, and DD Boost devices.

The *EMC NetWorker Data Domain Deduplication Devices Integration Guide* provides details on DD Boost devices.

**Table 24** Differences between disk devices

Function or operation	File type device (FTD)	Advanced file type device (AFTD)	DD Boost device
Create a device	<p>Device Property Window</p> <p>Select the media type: file.</p> <p>UNIX/Linux storage node: local or NFS only.</p> <p>Windows storage node: local path only. CIFS is not supported for FTDs</p>	<ul style="list-style-type: none"> <li>Device Configuration Wizard</li> <li>Device Property Window</li> <li>Select media type: adv_file.</li> <li>UNIX/Linux storage node: local or NFS only.</li> <li>Windows storage node: local or CIFS using UNC path or using NFS; Remote user, Password.</li> </ul>	<ul style="list-style-type: none"> <li>Device Configuration Wizard</li> <li>Device Property Window</li> <li>Select media type: Data Domain</li> </ul>
Storage location	Specified in the Name attribute.	Specified in the Device Access Information attribute.	Specified in the Device Access Information attribute.
Concurrent operations: <a href="#">Recover savesets by using AFTD concurrent operations on page 171</a> provides more information.	No	Yes	Yes
Reclaiming or recovering space	The nsrim program removes both aborted and expired save sets, once every 24 hours, following completion of a savegroup (if you have set volume recycle to Auto).	<ul style="list-style-type: none"> <li>Aborted save sets immediately removed.</li> <li>The nsrim program removes expired save sets from the media database once every 24 hours, following completion of a savegroup (if you have set volume recycle to Auto). NetWorker removes space on the AFTD as specified in the Reclaim Space Interval of the staging policy.</li> </ul>	<ul style="list-style-type: none"> <li>Reclaims only data that is unique, not required by other existing backups.</li> <li>NetWorker does not immediately remove aborted save sets, but marks them recyclable. A restarted save can be deduplicated. Otherwise, NetWorker removes the aborted save set during the next Recover Space operation.</li> </ul>

**Table 24** Differences between disk devices (continued)

Function or operation	File type device (FTD)	Advanced file type device (AFTD)	DD Boost device
Volume default capacity for devices	If the file type device was used prior to setting the Volume Default Capacity attribute, the data for that file type device must be staged or cloned to another device.	Does not apply.	Does not apply.
AFTD Percentage Capacity	Does not apply.	A setting determines the capacity that NetWorker software should stop writing to an AFTD; spans from 1 to 100%.	Does not apply.
When file system or volume is full	<ul style="list-style-type: none"> <li>• Waiting message displayed if no writable volume available or until volume becomes available.</li> <li>• Volume marked full and is no longer available for backups until the volume becomes appendable.</li> </ul>	<ul style="list-style-type: none"> <li>• Message displayed stating file system requires more space.</li> <li>• The nsrim program invoked to reclaim space for expired save set on AFTD.</li> <li>• Notification sent by email stating device is full.</li> <li>• Device waits until space become available. The volume is never marked as full.</li> </ul>	Backup to a DD Boost device fails and stops when full.
Save set continuation	Yes	No. Save sets that start on an AFTD must be completed on the same device.	No. Save sets that start on a DD Boost device must be completed on the same device.
Data format in device	EMC Open Tape Format (OTF).	Save stream (uasm) format (uses less space).	Deduplicated
Cloning operations	Save sets are cloned one at a time. Both automatic and manual cloning can begin only after all the save sets in a savegroup are backed up.	Save sets are cloned one at a time. Automatic cloning begins after the save sets are backed up. Manual cloning of a save set can begin as soon as it has finished its backup. Two simultaneous clone operations can be run from the command prompt, provided no backup,	The <i>EMC NetWorker Data Domain Deduplication Devices Integration Guide</i> provides details for advanced CCR cloning and replication with DD Boost devices.

**Table 24** Differences between disk devices (continued)

Function or operation	File type device (FTD)	Advanced file type device (AFTD)	DD Boost device
		recover, or stage operations run at the same time. The syntax is as follows: nsrclone -S [ssid/cloneid1] nsrclone -S [ssid/cloneid2]	
Client Direct backup: the storage node manages the devices for the NetWorker clients, but the clients send their backup data directly to the devices via network access, bypassing the storage node.	No.	Yes. Clients send their own backup data directly to the storage devices. If Client Direct backup is not available, a traditional storage node backup is performed.  NetWorker archive operations are not supported for Client Direct backup.	Yes. Clients use DD Boost DSP functionality to deduplicate their own backup data before sending it directly to the storage devices. If Client Direct backup is not available, a traditional storage node backup is performed.  NetWorker archive operations are not supported for Client Direct backup.

## File type devices

File type devices (FTDs) are legacy devices and their use is limited. Continued support for legacy and test purposes is maintained, however you are encouraged to use AFTD or DD Boost devices in preference to FTD. An FTD can be configured on the NetWorker server by creating a new Device resource in the same manner as for other storage devices.

The following conditions and restrictions apply to FTDs:

- The upper limit of save set size on an FTD may be either:
  - The upper limits supported by the operating system
  - The file size specified by the disk device vendor
- If multiple FTDs are configured on a system, each device must have a unique name.
- To use multiple FTDs on the same disk, partition the disk and create only one FTD per partition.
- Dynamic Drive Sharing is *not* supported.
- For FTDs created on a UNIX or Linux network file system (NFS):
  - The file system used for the FTD must not be used for any other data.
  - There must be one FTD per NFS system.
  - The Volume Default Capacity attribute for the FTD must be set to a size that is less than 100 percent of the total capacity of the file system.

**NOTICE**

Data loss will result if a full FTD is made appendable while a backup is pending completion and a save set is partially written to the full FTD. In this case, the partial save set (currently in “incomplete” state) will be overwritten.

## FTD capacity issues

For FTDs, the Volume Default Capacity is a hard limit on the amount of data that can be written to the device. The Volume Default Capacity value is an estimate of what the volume capacity is likely to be. If the value is not set correctly, the NetWorker percent-used calculation will be incorrect.

**Note**

By contrast, AFTDs ignore the Volume Default Capacity value to allow dynamic expansion of disk space.

The Volume Default Capacity attribute displays on the Configuration tab of the Device properties when Diagnostic Mode (View > Diagnostic Mode) is enabled:

- To avoid accidentally filling an FTD, set the Volume Default Capacity attribute to restrict the size of the device. For example, if a capacity of 100 MB is set, then the device will be marked full when 100 MB is reached.
- Volume Default Capacity attribute must not be set to a value of more than 4 TB.
- If the Volume Default Capacity of a volume changes, the changes do not take effect until the FTD is re-created, the directory contents are deleted, and the volume is relabeled.

**NOTICE**

If the FTD is used before the Volume Default Capacity attribute is set, then the legacy data on that FTD must be staged or cloned to another device. Otherwise, this data will be overwritten.

## Full FTD prevention

To prevent the file system from becoming full when backing up data to FTDs, policies can be used to move the data off the disk as soon as necessary. Save sets from FTDs can be staged or cloned to an AFTD to take advantage of advanced file type device features.

To make space for additional backups:

- Configure a save set staging policy. [Save set staging on page 342](#) provides details.
- Review and, if required, modify the retention policy of the save sets.

## Advanced file type devices

Advanced file type devices (AFTDs) overcome the main restrictions of traditional file type device (FTD) storage. AFTD storage is designed for large disk storage systems that use a volume manager to dynamically extend available disk space if the disk runs out of space during backup.

The *EMC Software Compatibility Guide* provides a list of supported volume managers.

## Memory requirements for AFTD backups

The physical memory requirements for a NetWorker storage node and Client Direct client depends on the peak AFTD usage.

The following is the list of physical memory requirements for AFTD:

- Allowing for other types of devices and services on a typical storage node, a storage node should have a minimum of 8 GB of RAM to host AFTDs.
- AFTD clients require a minimum of 4 GB of RAM at the time of backup to ensure optimum performance for Client Direct backups. Client Direct backups require client access to the AFTDs on either a CIFS or NFS network.
- Each AFTD requires an initial 24 MB of RAM on the storage node and Client Direct client. Each AFTD save session requires an additional 24 MB. To run 10 sessions requires  $24 + 240$  MB. The default max sessions of 60 sessions per AFTD requires  $24 + 1440$  MB.

## Create and configure an AFTD

You can create an AFTD by using either the Device Wizard or the device properties window.

### Creating an AFTD by using the Device Wizard

If you are creating an AFTD to use the client direct feature, see [Considerations for Client Direct clients on page 165](#) for information about specifying network path information when creating the AFTD.

#### Procedure

1. In the NMC **Enterprise** view, double-click the NetWorker managed application to launch its window.
2. In the **NetWorker Administration** window select the **Devices** view.
3. Verify that the path to the storage directory that will contain the AFTDs is allowed.
  - a. In the navigation tree select **Storage Nodes**.
  - b. Right-click the storage node that you will use and select **Properties**.
  - c. In the **AFTD allowed directories** list, verify or type the path of the storage directory that will contain the AFTDs.
  - d. Click **OK**.
4. In the navigation tree, right-click **Devices**, and select **New Device Wizard**.
5. In the **Select the Device Type** window, select **AFTD** and click **Next**.
6. In the **Select Storage Node** window, specify the path to the storage directory that will contain the AFTDs.
  - a. In the **Storage Node** list, select the storage node that you will use.
  - b. If the directory for the intended AFTDs is on a different storage node or a remote storage system, select **Device storage is remote from this Storage Node** and type the **Network Path** of the remote host directory that will contain the devices.

For example, if your storage node is a Microsoft Windows system and you will use a CIFS AFTD on a remote storage system host, this path could be something like the following:

```
\dzone1_storhost2.lss.corp.com\share-1
```

This storage path is *not* a device. It is the directory location in which the shared devices are to be created.

7. In **Browse or Manual**, select which option you will use to specify the pathnames of the devices:

- **Browse Storage Node or network path.** The next wizard step will prompt you to browse and add the devices.
- **Manually enter local or remote device paths.** Select this to skip the browse step and manually type unique names for the devices you want to add:
  - For remote devices, type the device paths relative to the Network Path that you specified for the storage directory. For example:  
cifsaftd-1  
cifsaftd-2
  - For local devices, type the absolute paths to these devices. For example:  
C:\cifsaftd-1  
C:\cifsaftd-2

[Multiple devices for a single volume configuration on page 167](#) provides details for shared volumes.

8. If the storage host is remote from the storage node, in the **Authentication** area, type the appropriate **Username** and **Password** to access the storage directory.

9. Click **Next**.

10. If you selected the **Browse** option in the previous window:

- a. In the **Select the Device Path** window, verify that your storage node shows the path of a storage directory.
- b. Add devices to the storage directory by clicking **New Folder** and typing unique device names. For example:  
cifsaftd-1  
cifsaftd-2
- c. Select the new devices to add and click **Next**.

11. In the **Configure Device Attributes** window, specify the attributes. If you added multiple devices in the previous window, select each device individually and specify its attributes:

- a. In **NetWorker Device Name**, type a unique name for the AFTD device.

For example, for a device on the NetWorker server host storage node:  
aftd-1

If you configure the device on a storage node host that is not the NetWorker server host, it is a “remote device” and this attribute must be specified with rd= and a colon (:) in the following format (for Microsoft Windows):

```
rd=remote_storagenode_hostname:device_name
```

For example:

```
rd=dzone1_storhost2:aftd-1
```

- b. (Optional) Add a comment in the **Comment** field.
- c. If Client Direct backup will be used, follow the details in [Considerations for Client Direct clients on page 165](#).
- d. In **Target Sessions** specify the number of sessions that a nsrmmmd data mover process on the device will handle before another device on the host will take the additional sessions. Use this setting to balance the sessions among nsrmmmd processes.  
If another device is not available, then another nsrmmmd process on the same device will take the additional sessions.  
Typically, set this attribute to a low value. The default value is 4 for AFTDs. It may not be set to a value greater than 60.
- e. In **Max Sessions** specify the maximum number sessions the device may handle. If no additional devices are available on the host, then another available storage host takes the additional sessions, or retries are attempted until sessions become available.  
The default value is 32 for AFTDs, which typically provides best performance. It cannot be set to a value greater than 60.

---

**Note**

The **Max Sessions** setting does not apply to concurrent recover sessions.

- f. Click **Next**.
12. In the **Label and Mount device** window, if you select the **Label and Mount** option, specify the attributes for:
  - **Pool Type**.
  - **Pool to use**.
13. In the **Review the Device Configuration** window, review the settings and click **Configure**.
14. In the **Check results** window, review whether the devices were successfully completed or any messages. Click **Finish**, or to go back, click **Back** or the appropriate wizard step.

## Creating an AFTD by using the Properties window (Linux and UNIX)

### Procedure

1. Create one directory for each disk (or partition) to be used for an AFTD.  
AFTDs require a directory (folder) to be created in the disk file system that the NetWorker server or storage node recognizes as the device name (and the destination for the data).
- NOTICE**
- Do not use a temporary directory for NetWorker disk file devices. The data could be overwritten.
2. In the server's **Administration** interface, click the **Devices** view.
  3. Verify that the path to the storage directory that will contain the AFTDs is allowed.
    - a. In the navigation tree select **Storage Nodes**.
    - b. Right-click the storage node that you will use and select **Properties**.
- 160 EMC NetWorker 8.2 Administration Guide

- c. In the **AFTD allowed directories** list, verify or type the path of the storage directory that will contain the AFTDs.

AFTDs can be created and accessed only by these listed paths. If this list is left empty, there are few restrictions as to where a device path can be created.

- d. Click **OK**.

4. In the navigation tree, right-click **Devices** and select **New**.

The Create Device window opens, with the General tab selected. The Identity area might show a default device name in the Name field.

5. In the **Identity** area, set the following attributes:

- a. In the **Name** attribute, type the name of the directory you created for the AFTD.

For example:

aftd-1

If you configure the device on a storage node host that is not the NetWorker server host, it is a remote device and this Name attribute must be specified with rd= in the following format (for Microsoft Windows):

rd=remote\_snode\_hostname:device\_name

For example:

rd=snode-1:aftd-1

- b. (Optional) Add a comment in the **Comment** field.

- c. In the **Device Access Information** attribute, provide complete paths to the device directory.

For non-root or cross-platform Client Direct access:

For non-root or cross-platform Client Direct access to an AFTD, do not specify an automounter path or a mounted path. Instead, specify the path in the host:/path format, even if the AFTD is local to the storage node, for example:

NFS\_host:/path

Where

- NFS\_host is the hostname of the NFS file server
- path is the NFS-mountable path exported by the file server  
This format is required to allow Client Direct access for Windows or non-root Unix clients.

#### Note

Non-root Client Direct access to an NFS AFTD is supported only with the NFSv3 protocol and AUTH\_SYS authentication on the NFS host.

For root-only Client Direct Access

For Client Direct access to an AFTD when the backup client is able to run as root on the AFTD host, provide a mount point or automounter path, for example, for an NFS-mounted device:

/mnt/aftd-1

/net/storho-1/snode-1/aftd-1

Where:

- aftd-1 is the storage device directory name

- storho-1 is the storage system hostname
- snode-1 is the storage node hostname  
The first path enables the storage node to access the device via its defined mount point. The second path enables Client Direct clients to use the automounter path to directly access the device, bypassing the storage node.

d. In the **Media Type** field, select adv\_file, for the AFTD.

[Considerations for Client Direct clients on page 165](#) provides additional details for Client Direct configurations.

[Multiple devices for a single volume configuration on page 167](#) provides additional details for shared volumes.

6. In the **Status** area, ensure that the **Auto Media Management** tape feature is enabled.
7. In the **Cleaning** area, leave the options for cleaning at their default (disabled) settings, so that automatic cleaning is invoked.
8. Select the **Configuration** tab.
9. In the **Save Sessions** area, set the number of concurrent save sessions (streams) and the number of nsrmmmd (data mover) processes the device may handle:
  - **Target Sessions** is the number of sessions that a nsrmmmd process on the device will handle before another device on the host will take the additional sessions. Use this setting to balance the sessions among nsrmmmd processes.  
If another device is not available, then another nsrmmmd process on the same device will take the additional sessions.  
Typically, set this attribute to a low value. The default values are 4 for AFTDs and 6 for DD Boost devices. It may not be set to a value greater than 60.  
[Multiple devices for a single volume configuration on page 167](#) provides details on volume sharing.
  - **Max Sessions** is the maximum number sessions the device may handle. If no additional devices are available on the host, then another available storage host takes the additional sessions, or retries are attempted until sessions become available.  
The default values are 32 for AFTDs and 60 for DD Boost devices, which typically provides best performance. It cannot be set to a value greater than 60.  
The Max Sessions setting does not apply to concurrent recover sessions.
  - **Max nsrmmmd count** limits the number of nsrmmmd processes that can run on the device. Use this setting to balance the nsrmmmd load among devices. The default value is 4.  
To modify this value, first adjust the sessions attributes, apply and monitor the effects, then update max nsrmmmd count.  
At least one nsrmmmd process will always be reserved for restore or clone operations.
10. In the **Local Backup** area, leave **Dedicated Storage Node** at **No** (the default).
11. In the **Remote Host** area, if an NFS path is specified in the **Device Access Information**, then type a **Remote User** name and **Password**.

The remote user name is the name of the user on the NFS server. It is recommended that you also specify the numeric user id (UID) of that user. Do this by appending a colon (:) and the UID after the user name, for example, user\_name:4242.

**Note**

If the device username is changed after labeling, manual action may be required to change the owner of all files and directories in the AFTD. NetWorker will attempt to make this change automatically during the next operation, however the ability to do so depends on the security configuration of the file server where the AFTD storage resides.

12. Click **OK** when the configuration is complete.
13. If a new password for an AFTD is provided, unmount and re-mount the device to ensure that the change takes effect.

## Creating an AFTD by using the Properties window (Windows)

You can configure an AFTD on a storage node running Microsoft Windows.

### Procedure

1. Create one directory for each disk (or partition) to be used for an AFTD. AFTDs require a directory (folder) to be created in the disk file system that the NetWorker server or storage node recognizes as the device name (and the destination for the data).

**NOTICE**

**Do not use a temporary directory for AFTDs. The data could be overwritten.**

2. In the server's **Administration** interface, click the **Devices** view.
3. Verify that the path to the storage directory that will contain the AFTDs is allowed.
  - a. In the navigation tree select **Storage Nodes**.
  - b. Right-click the storage node that you will use and select **Properties**.
  - c. In the **AFTD allowed directories** list, verify or type the path of the storage directory that will contain the AFTDs.

AFTDs can be created and accessed only by these listed paths. If this list is left empty, there are few restrictions as to where a device path can be created.

4. In the navigation tree, right-click **Devices** and select **New**. The Create Device window opens, with the General tab selected. The Identity area might show a default device name in the Name field.
5. In the **Identity** area, set the following attributes:

- a. In the **Name** attribute, type the name of the directory that you created for the AFTD.

For example:

aftd-1

If you configure the device on a separate storage node host that is not the NetWorker server host, it is a remote device and this Name attribute must be specified with rd= in the following format:

rd=remote\_snode\_hostname:device\_name

For example:

rd=snode-1:aftd-1

- b. (Optional) Add a comment in the **Comment** field.

- c. In the **Device Access Information** attribute, provide complete paths to the device directory. You can provide alternate paths for the storage node and for Client Direct clients, for example:

- For an AFTD on the storage node's local disk, which it shares via CIFS:  
E:\aftd-1

\snode-1\aftrd-1

The first path enables the storage node to access the device via its local drive. The second path enables Client Direct clients to directly access the device, bypassing the storage node.

- For a CIFS-mounted AFTD, specify the complete paths of the directory created by using the Universal Naming Convention (UNC), for example:  
\CIFS\_host\share-point-name\path
- To enable UNIX/Linux clients to use this AFTD for Client Direct access, you must provide a NFS path in the host:/path format, for example:  
NFS\_host:/path

where:

- NFS\_host is the hostname of the NFS file server
- path is the NFS-mountable path exported by the file server

- d. In the **Media Type** field, select adv\_file, for the AFTD.

[Considerations for Client Direct clients on page 165](#) provides additional details for Client Direct configurations.

[Multiple devices for a single volume configuration on page 167](#) provides additional details for shared volumes.

6. In the **Status** area, ensure that the **Auto Media Management** tape feature is *not* enabled.

7. In the **Cleaning** area, leave the options for cleaning at their default (disabled) settings, so that automatic cleaning is not invoked.

8. In the **Save Sessions** area, set the number of concurrent save sessions (streams) and the number of nsrmmmd (data mover) processes the device may handle:

- **Target Sessions** is the number of sessions that a nsrmmmd process on the device will handle before another device on the host will take the additional sessions. Use this setting to balance the sessions among nsrmmmd processes.

If another device is not available, then another nsrmmmd process on the same device will take the additional sessions.

Typically, set this attribute to a low value. The default values are 4 for AFTDs and 6 for DD Boost devices. It may not be set to a value greater than 60.

[Multiple devices for a single volume configuration on page 167](#) provides details on volume sharing.

- **Max Sessions** is the maximum number sessions the device may handle. If no additional devices are available on the host, then another available storage host takes the additional sessions, or retries are attempted until sessions become available.

The default values are 32 for AFTDs and 60 for DD Boost devices, which typically provides best performance. It cannot be set to a value greater than 60.

The Max Sessions setting does not apply to concurrent recover sessions.

- **Max nsrmmmd count** limits the number of nsrmmmd processes that can run on the device. Use this setting to balance the nsrmmmd load among devices. The default value is 4.

To modify this value, first adjust the sessions attributes, apply and monitor the effects, then update max nsrmmmd count.

At least one nsrmmmd process is reserved for restore or clone operations.

9. In the **Local Backup** area, leave **Dedicated Storage Node** at **No** (the default).
10. In the **Remote Host** area, if a network path is specified in the **Device Access Information**, then type a **Remote User** name and **Password**.
11. Click **OK** when the configuration is complete.
12. If a new password for an AFTD is provided, unmount and re-mount the device to ensure that the change takes effect.

## Device target and max sessions default values and ranges

There are default values and ranges for device target and max sessions in the NetWorker Administration interface.

The following table lists the default values for target and max sessions values.

**Table 25** Default values and ranges for target and max sessions attributes

Device type	Default target sessions	Default max sessions	Recommended sessions*	Range
AFTD (traditional storage)	4	32	1 - 32	1 - 512
AFTD (including Data Domain CIFS/NFS)	4	32	1 - 10	1 - 512
Data Domain (DD Boost)	6	60	1 - 10	1 - 60
Cloud	1	512	Any	1 - 512
NDMP	4	512	1 - 32	1 - 512
FTD (traditional)	4	32	1 - 16	1 - 512
VTL/Tape (traditional)	4	32	1 - 16	1 - 512
VTL/Tape (Data Domain / Deduplicated)	4	32	1 - 1	1 - 512

\* The recommended session values are guidelines only and are subject to bandwidth, data type, and device capabilities.

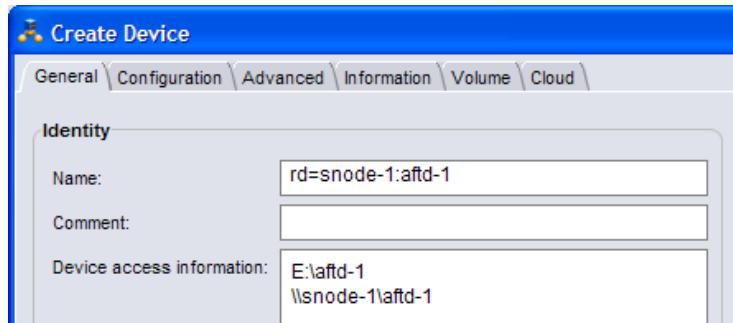
## Considerations for Client Direct clients

The Client Direct backup feature enables clients to back up directly to the storage devices, bypassing the storage node. The storage node manages the devices but does not handle the backup data. Device configuration for Client Direct clients depends on what type of storage device you will use and how it is connected to the storage nodes:

- Client Direct clients require a network connection and a remote network protocol to reach the storage device. Windows clients can use a CIFS or NFS path, although a CIFS path will generally yield better performance. UNIX clients must use a NFS path.
- If the storage device is to a NAS piece that is not directly attached to any storage node, the device access information (path) would be the same for all storage nodes and Client Direct clients.

- If the storage device is directly attached to a Windows storage node, then the storage node would use different device access information than the Client Direct clients. The device access information should specify multiple access paths to cover local and remote use cases. The following figure shows an example for a CIFS AFTD.

**Figure 10** Example name and CIFS access information.



- As of NetWorker 8.1, non-root and cross-platform Client Direct backups to AFTDs are now supported for NetWorker clients on UNIX/Linux or Microsoft Windows. The AFTD can be managed by a Linux/UNIX or a Windows storage node. The AFTD can be local or mountable on the storage node. To configure such a device, you must:
  - Specify a NFS path in the AFTD's Device access information attribute. Specify the path using the NFS\_host:/path format. Use this format whether or not the AFTD is local to the storage node or mountable on the storage node. Non-root UNIX/Linux NetWorker clients require this NFS format for Client Direct access.
    - You can also specify a CIFS path for Windows Client Direct backups. A CIFS path generally yields better backup performance than a NFS path for Windows Client Direct backups. If you are setting up an AFTD on a Windows storage node, specify the CIFS path first, for example:  
\\fileserver\aftrd1  
fileserver:/aftrd1  
If you are setting up a UNIX/Linux storage node, specify the NFS path first, for example:  
fileserver:/aftrd1  
\\fileserver\aftrd1
  - Specify the user name and password that is required to access the storage server on which the AFTD resides. Enter the user name and password in the Remote User and Password attributes in the NetWorker AFTD device resource.
  - The NFS server that provides AFTD storage must permit access using the NFSv3 protocol with AUTH\_SYS (AUTH\_UNIX) authentication.
  - The NFS server that provides AFTD storage must not restrict access to clients by using only privileged ports.

#### Note

When using a NetWorker version 8.1 server with an earlier version of a NetWorker storage node, it is possible to configure an AFTD using the new NFS path format (NFS\_host:/path). However, this path will not work correctly because the older-version storage node does not have the required NFS support.

- Checkpoint restart does not support Client Direct backups to DD Boost devices. If a client is enabled for checkpoint restart and a Client Direct backup is attempted to a

DD Boost device, then the backup reverts to a traditional storage node backup instead.

- For Client Direct backups to AFTDs, checkpoint restart points are not made less than 15 seconds apart. Checkpoints are always made after larger files that require more than 15 seconds to back up.
- Archive operations are not currently supported for Client Direct backups.

## Multiple devices for a single volume configuration

In some environments, a configuration of multiple devices that share a single NetWorker storage volume can result in performance gains. For example, a read or write request can be sent to the storage node that is closest to the requestor. However, for some use cases and environments concurrent read/write operations to a single volume from many storage nodes could result in disk thrashing that impacts performance.

Multiple devices can be created on separate storage nodes or on the same storage node. Each device must be created separately, have a different name, and must correctly specify the path to the storage volume location.

For example, if you create three devices, one on the NetWorker server host named “dzone1” (that uses the server’s local storage node) and two remote devices (rd) on remote storage nodes, the Name attributes for the three devices, each created separately, might be specified by different aliases as follows:

```
aftd-1a  
rd=dzone1-sn2:aftd-1b  
rd=dzone1-sn3:aftd-1c
```

The Device Access Information for each of these aliases would specify a single directory that must be specified as a valid complete path. For example, if a directory is named “aftd-1” on the storage host named “storho1,” the path might be specified as follows:

- If the storage node uses an automounter:  
/net/storho1/dzone1/aftd-1
- If the storage node uses an explicit system mountpoint, you might specify one of the following paths:
  - /mnt/storho1/dzone1/aftd-1
  - /mnt/dzone1/aftd-1
  - storho1:/dzone/aftd-1

## AFTD concurrent operations and device formats

The following operations can be performed concurrently on a single storage node with an AFTD:

- Multiple backups and multiple recover operations
- Multiple backups and one manual clone operation
- Multiple backups and one automatic or manual staging operation

It might be required to increase the server parallelism value to complete the concurrent operations with an AFTD device when the number of simultaneous save sessions reaches the maximum value for server parallelism.

For example, if server parallelism is set to 4, and there are 4 simultaneous saves going to an AFTD, set the server parallelism to 5 to complete a concurrent clone/stage operation from this AFTD while the four saves are in progress.

---

**Note**

Starting with NetWorker 8.0, multiple clone sessions can be run from a single AFTD or DD Boost device if each clone is written to a dedicated tape device. However, the number of clone sessions that can be run is limited by the value in the device's max nsrmmd count attribute. [Create and configure an AFTD on page 158](#) provides more information.

---

## Labeling and mounting an AFTD

If there are multiple volumes in the pool, you can select an available volume to associate with the device.

### Procedure

1. Right-click the AFTD storage device and select **Label**.

The Label dialog box appears.

2. In the Pools field, select the media pool to be used for the device.

A label for the storage device is generated and displays in the Volume Label field. The label name is based on the label template for the selected pool.

It is recommended to use a pool dedicated to AFTD backup devices only.

**NOTICE**

If an existing volume is re-labeled, a warning is issued. The data previously stored on the volume will be lost and this action cannot be undone. Mounting the volume without labeling provides access to previous data.

---

3. Select **Mount after labeling** and click **OK**.

## Insufficient AFTD disk space

When an AFTD runs out of disk space, the current backup is interrupted and the following message displays:

```
Waiting for more available space on filesystem device-name
```

Immediately following the message, the action associated with the Filesystem Full – Recover adv\_file Space notification occurs. By default, the action for this notification uses the nsrim command to delete expired save sets. If enough space is cleared, the backup continues. If the recycle setting for the volume is manual, then the expired save sets are not removed from the volume.

The AFTD deletes expired save sets depending on the retention policy and the recycle setting. If sufficient storage space is not available after 10 minutes from when the expired savesets begin deletion, the associated Filesystem Full—Waiting for adv\_file Space notification action occurs. By default, an email notification is sent to the root user on the NetWorker server on UNIX and Linux, and a message is logged in the media log file in NetWorker\_install\_path\logs on Windows. [Viewing log files on page 677](#) provides information about viewing log files.

When the notification is sent, and the message is logged in the media log file, the backup stops until space is available for the backup to continue. You can create customized notifications to change and expand how the NetWorker software behaves when an AFTD Filesystem Full notification occurs. Custom notifications can also invoke custom scripts and other programs to expand the capacity of existing AFTDs. [Indexes on page 510](#) and

[Configuring NetWorker SNMP notifications on page 598](#) provides information on using notifications.

## Creating a custom notification to extend disk space

While the NetWorker default Filesystem Full — Recover adv\_file Space notification works by removing its expired save sets, a custom notification could be configured to expand disk or file system space in other ways.

### Procedure

1. In the server's **Administration** interface, click **Configuration**.
2. Right-click **Notifications** and select **New**.
3. For **Name**, type a unique name for this custom notification, such as First adv\_full notice.
4. For **Event**, clear all choices *except* adv\_file.
5. For **Priority**, clear all choices *except* Waiting.
6. For **Action**, specify the full path of the custom script configured to expand diskspace, for example: /mybin/my\_first\_custom\_script.
7. Click **OK**.

## Creating a custom notification for insufficient disk space

The NetWorker default Filesystem Full — Waiting for adv\_file Space notification works by sending an email notification, a custom notification could be configured to do whatever the user indicates. The wait time after the default notification is approximately 10 minutes.

### Procedure

1. In the server's **Administration** interface, click **Configuration**.
2. Right-click **Notifications** and select **New**.
3. For **Name**, type a unique name for this second custom notification, such as Second adv\_full Notice.
4. For **Event**, clear all choices *except* adv\_file.
5. For **Priority**, clear all choices except **Critical**, **Emergency**, and **Alert**.
6. For **Action**, specify the full path of the custom script to be invoked, for example: / mybin/my\_second\_custom\_script.
7. Click **OK**.

## AFTD device target and max sessions

The default settings for AFTD target sessions and max device sessions typically provide optimal values for AFTD performance:

- Device target sessions is 1
- Device max sessions is 32 to avoid disk thrashing

If required, both device target, and max session attributes can be modified to reflect values appropriate for the environment.

### Note

The Max Sessions setting does not apply to concurrent recover sessions.

## AFTD load balancing

You can adjust the target and max sessions attributes per device to balance the data load for simultaneous sessions more evenly across available devices. These parameters specify the maximum number of save sessions to be established before the NetWorker server attempts to assign save sessions to another device.

For AFTDs, all volumes, depending on the selection criteria (pool settings), choose the AFTD with the least amount of data written to it, and join sessions based on the device's target and max sessions. If the number of sessions being written to the first device exceeds the target sessions setting, another AFTD is considered for new backup sessions and is selected from the remaining suitable AFTDs. The AFTD that is selected will be the AFTD with the least amount of NetWorker data written to it. The least amount of data written is calculated in bytes (not by percentage of disk space used) and only bytes that were written by NetWorker are counted.

To ensure that a new session always writes to the AFTD with the least amount of data written to it, you can set each AFTD device's max sessions attribute to 1. However, setting the max sessions attribute to 1 may not be practical. Alternatively, set the target sessions attribute to 1. In this way, load balancing will occur on a best efforts basis.

## Space management for AFTD

A configurable setting for determining at what capacity the NetWorker software should stop writing to an AFTD spans from 1 to 100%. Setting the value to 0 or leaving the attribute empty in the AFTD Percentage Capacity attribute is equivalent to a setting of 100%. This means that the entire capacity of the filesystem can be used for the AFTD volume.

When set, the AFTD Percentage Capacity attribute is used to declare the volume full and to calculate high/low watermarks. When the percentage capacity attribute is modified, mount and re-mount the volume for the new settings to take effect.

The level watermark is calculated based on the percentage of restricted capacity, not on the full capacity of the filesystem.

In the Console Administration interface, the AFTD Percentage Capacity displays in the Configuration tab of the Properties window of a device when Diagnostic Mode is enabled. To enable Diagnostic Mode, select View > Diagnostic Mode.

### NOTICE

If your device uses compression or deduplication, you can still use the AFTD Percentage Capacity attribute however, the device will be marked as having reached its threshold prematurely. In this case, there will be more unused space on the disk than expected. This is because the threshold limit is based on the amount of data being protected without accounting for the effect of compression or deduplication.

## AFTD operation verification

The AFTD can be deployed in varying environments with local disks, and with NFS-mounted or CIFS-mapped disks. The configuration of this feature affects its operation. Ensure that the AFTD is fully operational in the production environment before deploying it as part of regularly scheduled operations.

As part of the validation process, test these operations:

- Backup
- Recover

- Staging
- Cloning
- Maximum file size compatibility between the operating system and a disk device
- Use of a volume manager to increase the file system size while the file system is in use
- File system behavior when the disk is full

Some versions of NFS and CIFS drop data when a file system becomes full. Be sure to use versions of NFS, CIFS, and operating systems that fully support full file systems. On some disk devices, the volume labeling process can take longer than expected. Labeling time depends on the type of disk device used and does not indicate a limitation of the NetWorker software. The upper limits of save set size depend on either the upper limits supported by the operating system or the file size specified by the disk device's vendor.

#### **NOTICE**

Do not edit device files and directories. This can cause unpredictable behavior and make it impossible to recover data.

---

## Changing the AFTD block size

The maximum potential block size for backups to an AFTD device can be adjusted. Larger block sizes for backups can improve backup speed under certain conditions. This is especially noticeable on remote AFTD devices that are not local to the storage node, for example, AFTDs that are connected with CIFS or NFS.

Changes to the maximum potential block size value for an AFTD device take effect only after the AFTD device is labelled. The minimum allowable block size is 128 kilobytes and the maximum block size is 256 kilobytes.

If you have an AFTD device that is performing backups slowly, try marking the device as read-only and create a new AFTD device with a block size between 128-256 kilobytes.

#### **NOTICE**

Changing the block size and re-labeling an existing AFTD has the potential to destroy data if the data is not staged to another location.

---

### Procedure

1. In the server's **Administration interface**, click **Devices**.
2. Select **View > Diagnostic Mode**.
3. Select **Devices** in the navigation tree. The Devices detail table appears.
4. Double-click the device in the devices table and select the **Advanced** tab.
5. In the **Device block size** attribute, select a value from 128 to 256.
6. Click **OK**.
7. Relabel the AFTD device for the new setting take effect.

## Recover savesets by using AFTD concurrent operations

When recovering from an AFTD, save sets are recovered concurrently. Multiple save sets can be simultaneously recovered to multiple clients. AFTD save sets can be cloned to two different volumes simultaneously. [File type devices on page 156](#) provides more information.

## Concurrent AFTD recovery operation limitations

AFTD concurrent recovery currently has these limitations:

- Not available to the Windows recover interface (`winworkr`). Use the `recover` command. The *EMC NetWorker Command Reference Guide* or the `recover` man page provides more information.
- Not available to nonfile recoveries, such as NDMP and NetWorker database modules.
- NetWorker release 7.2x clients on Windows recover data from AFTD storage nodes sequentially. Concurrent recoveries must be performed from the command line by using the `recover` command, either by using multiple `-S` options to identify multiple save sets, or executing multiple `recover` commands concurrently.

## Deactivate and erase an AFTD

You can deactivate an AFTD device so it does not interfere with normal backup operations. Use one of the following options:

- [Converting a device to read-only on page 172](#)
- [Disabling a device on page 172](#)
- [Deleting a device on page 173](#)

### Converting a device to read-only

Conversion of a device to read-only prevents the use of the device for backup operations. The device can still be used for read operations, such as restore and clone.

#### Procedure

1. In the **NMC** window for your NetWorker server, click the **Devices** view and select the **Devices** folder in the navigation tree.
2. In the **Devices** table, right-click the device to be converted to read-only and select **Unmount**.
3. Right-click this unmounted device and select **Properties**.
4. In the Device Properties window, select **Read only** and click **OK**.
5. Right-click the device and select **Mount**.

### Disabling a device

Disabling a device prevents further operation of the device. The device may be re-enabled to restore old data, which is retained but not active.

#### Procedure

1. In the **NMC** window for your NetWorker server, click the **Devices** view and select the **Devices** folder in the navigation tree.
2. In the **Devices** table, right-click the device to be disabled and select **Unmount**.
3. Right-click this unmounted device and select **Enable/Disable** to disable.
4. Inspect the **Enabled** column of the table to verify that the device is disabled.

## Deleting a device

The procedure for deleting a device includes an option for also erasing the volume (access path) that stores the device's data. The volume can be erased only if no other device in the system shares the volume.

### Procedure

1. In the NetWorker server **Device** view, click **Devices** in the navigation tree.
2. In the **Devices** table, right-click the device to be removed and select **Delete**.

A confirmation window appears.

3. In the confirmation window:

- To delete the device from the NetWorker configuration only, without erasing the device's data, click **Yes**.
- To delete the device and erase the device's data and volume access path, select the **Permanently erase all data and remove media and index information for any selected AFTDs or Data Domain devices** option, and click **Yes**.

---

### Note

If the volume that you want to erase is shared by another device, then an error message displays the name of the other device. You must delete all other devices that share the volume until the last one remaining before you can erase the volume.

4. If the device is mounted or the device is a member of a pool, then a second confirmation window displays the details of the device and pool. To confirm the device unmount, the removal of the device from the pool, and the deletion of the device, click **Yes**.

## DD Boost devices

DD Boost devices are covered separately in the *EMC NetWorker Data Domain Deduplication Devices Integration Guide*.

## Cloud devices

This section describes how to configure the NetWorker Cloud Backup Option (NCBO) to perform backup, staging, cloning, and recovery operations to cloud configurations. Backups to cloud occur over a TCP/IP network and can be compressed and encrypted. NetWorker supports EMC Atmos-based cloud storage. More information on Atmos is available at <http://www.emc.com>.

## Cloud backup devices compared to other device types

NetWorker backup, staging, cloning, and recovery to cloud storage devices are similar to those operations that are performed with conventional devices. However, cloud devices also have unique features.

The following table lists the major similarities with other backup device types as well as the unique features of a cloud storage device.

**Table 26** A comparison of cloud devices to other device types

Feature	Cloud backup device	AFTD device	Tape device
Same volume mounted simultaneously on multiple devices	Yes	No	No
Staging source	No	Yes	No
Staging destination	Yes	Yes	Yes
Cloning	Yes	Yes	Yes
Auto mount and unmount	Yes	No	Yes *
Data transformation engine (enables encryption and compression on storage node)	Yes	No **	No **

\* When the tape is controlled by a tape library.  
\*\* Encryption and compression can still be enabled through NetWorker client side directives.

## Cloud backup requirements and considerations

The following conditions must be met before you can backup to the cloud:

- The NetWorker Cloud Backup Option must be licensed and enabled. The *EMC NetWorker Licensing Guide* provides information about licence enablers.
- The NetWorker Cloud Backup Option is supported on Windows and Linux storage nodes only.
- An Atmos cloud account is set up and you have a username and password to access the cloud account. The *EMC Atmos Installation Guide* and the *EMC Atmos System Management GUI Guide* provides information about setting up and managing an Atmos account.
- If the Atmos server and the NetWorker server are separated by a firewall, TCP ports 80 and 443 must be open to allow outgoing communication from the NetWorker server to the Atmos server. If a proxy server is configured in the environment, a firewall exception may also need to be created to ensure unrestricted access. If these ports are not open, device operations will fail with the following error:

```
Atmos label operation failed: Failed to write cloud label:  
Couldn't connect to server.
```

Be aware of the following considerations with respect to cloud support:

- NetWorker Avamar deduplication storage nodes do not support cloud backups.
- For NDMP, only a Data Server Agent (DSA) is supported for cloud backups.
- NetWorker versions prior to 7.6 do not support cloud backups.

## Cloud best practices

Consider the topics and recommendations in this section before implementing cloud backups.

## Direct NetWorker client backups to a cloud storage device

You direct client backups to a cloud storage device using media pools, in the same way you would direct any other client backup to a device or set of devices. However, be aware of the following recommendations:

- Set up a media pool for cloud storage devices and give the pool a unique label template.
- Do not mix cloud backup devices with other types of backup devices in a media pool. [Sorting Backup Data on page 283](#) provides information about setting up media pools.

## Concurrent backup and recovery operations

A single cloud volume can be mounted on multiple cloud storage devices to support concurrent backup and recovery operations. For example, to optimize performance you could mount cloud volume A on three cloud storage devices: one for backup (device CL1), one for recovery (device CL2), and one for clone operations (device CL3). There is no limit to the number of cloud storage devices that can be mounted on a single cloud volume. Consider such an approach to optimize backup and recovery performance.

## Network dependencies

Cloud backups are highly dependent on the network connection that is used to access the cloud service. Any disruption in connectivity or a slowdown in network access speed may adversely affect cloud backups or recoveries.

## HTTPS communications with the Cloud server

NetWorker enables you to use https to securely communicate with the Cloud server.

Configure https communications when you configure the cloud device in NetWorker. You will need to retrieve the SSL certificate for the Cloud server before you create a new device or modify an existing cloud device. Use the nsrssltrust command on the NetWorker server to retrieve the SSL certificate of the Cloud server and store the certificate to a local file.

To retrieve the certificate file, type the following command:

```
nsrssltrust -c path\filename -u https_server
```

where:

*path\filename* is the location to store the certificate file on the NetWorker server.

*https\_server* is the hostname of the https server.

For example:

```
nsrssltrust -c ./atmos1.cert -u https://accesspoint.atmosonline.com:  
443
```

## Create and label a cloud storage device

It is required to create and label cloud storage devices for use with the NetWorker software.

This section contains the following topics:

- [Creating the cloud storage device on page 176](#)

- [Labelling and mounting the cloud storage device on page 178](#)

## Creating the cloud storage device

### Procedure

1. In the server's **NetWorker Administration** interface, click **Devices**.
2. Right-click **Devices** in the navigation tree, and select **New**. The **Create Device** window appears, with the **General** tab selected, and a default device path in the **Name** field of the **Identity** area of the window.
3. In the **Name** field, replace the default name with a name that uniquely identifies the cloud storage device. If the device is configured on a remote storage node, indicate that the storage node is remote, by including *rd=hostname:* in the name. For example, if the remote storage node is neptune, then the device path might be *rd=neptune:cloud1*.

---

### Note

A cloud storage device name does not specify a path to the device. You can use any combination of alphanumeric characters for the device name.

---

4. In the **Comment** field and the **Description** field, add an optional comment and description, respectively.
5. In the **Media Type** field, select Atmos COS as the device type if you are using Atmos as the cloud server.
6. In the **Remote User** field, type the username that is used to access the cloud server. For an Atmos COS device, this is the token-id.
7. In the **Password** field, type the password that is used to access the cloud server. For an Atmos device, this is the shared secret.
8. Select the **Cloud** tab to specify additional information specific to the cloud backup device.
9. In the **Server** field, type the IP address or fully qualified domain name of the cloud server.
10. Use the Parameter options to adjust network communication attributes:
  - a. In the **Network Write Size** field, specify the amount of backup data, in kilobytes, to cache in memory before sending to the cloud. Larger write sizes typically result in better performance but results vary depending on the underlying network characteristics. Also be aware that larger sizes consume more memory on the storage node for the duration of the backup or recover operation.
  - b. In the **Number of Retries** field, specify the number of times that NetWorker will attempt to send backup or receive recover data in the event of a network failure.
  - c. In the **Send/Receive Timeout** field, specify the number of seconds that NetWorker will wait for confirmation that network send and receive transmissions to the cloud server have occurred successfully. If the timeout period expires, the data transmission is considered to have failed.
    - Set the value of this field in conjunction with the Network Write Size field. Larger Network Write Size values require larger Send/Receive Timeout values to avoid failures. Optimal values for the Send/Receive Timeout field vary depending on the network speed and bandwidth.
    - The save group's Inactivity Timeout value can potentially interact with the Send/Receive Timeout value in unintended ways. To avoid this possibility,

ensure that the save group's Inactivity Timeout value (default is 30 minutes) is greater than the Send/Receive Timeout value (default is 30 seconds).

- d. In the **Network Failure Retry Interval** field, specify the number of minutes that a backup or recover session must wait before a failed network connection results in an aborted backup or recover session.
11. In the **Compression** field, select a compression level for data that is sent to the cloud. Faster compression speeds result in less data compression but also require less CPU resources. The fastest compression speed, Compression Speed Fast, performs the least amount of data compression and is selected by default.

To choose an optimal compression value, balance the potentially longer backup window of using a slower compression speed against the potential efficiency and cost savings of sending less backup data to the cloud.

**NOTICE**

If the NetWorker Cloud Back Option determines that backup data cannot be compressed effectively, compression may not occur regardless of the setting in this field.

12. In the **Encryption** field, specify whether to enable or disable encryption of data sent to the cloud. Encryption is standard NetWorker AES 256 bit encryption and is selected by default. If desired a NetWorker datazone pass phrase can be defined that would be used to recover encrypted data.

If this option is selected, encryption will occur regardless of any client-side encryption directives. For more information about encryption including how to specify a new datazone pass phrase, refer to [Backup data encryption on page 102](#).

**NOTICE**

If encryption is already enabled for the NetWorker client and encryption is enabled in this field, backups will be slower because encryption functions will occur twice.

13. Use the **Cloud network interface** field if the Storage node has multiple network interfaces. If it does, specify the IP address of the network interface that will send backup data to the cloud.

To display the Cloud network interface field, select View>Diagnostic Mode from the menu bar.

14. Select **Throttling** and then click the Bandwidth icon  to display a dialog box where you can adjust the maximum internet bandwidth that a cloud backup or recovery operation can consume at any given time of the day or week. This option enables you to prevent network congestion by limiting cloud backup and recovery activity during peak internet usage.

- a. Select **New** to add a bandwidth throttling policy.
- b. From the **Day** field, select the day of week to which the policy applies.
- c. Click the up and down arrows to select a time of the day to which the policy starts and ends. Alternatively, type the times directly into the **Start time** and **End time** fields.
- d. Click the up and down arrows to select the maximum possible network bandwidth, in megabits per second, that a backup or recovery operation can consume when the policy is in effect. Alternatively, type the values directly in the fields.

You can create as many policies per day as required. You can also modify or delete existing throttling policies as necessary.

15.Click **OK** when the configuration is complete.

## Labelling and mounting the cloud storage device

If there are multiple cloud volumes, you will be able to select the volume to associate with the cloud storage device.

### Procedure

1. Select the cloud storage device, right-click and select **Label**. The **Create new cloud volume** dialog box appears.
2. In the Pools field, select the media pool to be used for cloud storage devices.

---

### Note

It is recommended that the media pool you select be used for cloud backup devices only.

A label for the cloud storage device is generated and displayed in the Volume Label field. The label name is based on the label template that was specified for the cloud media pool.

3. Select **Mount after labeling** and click **OK**.

## Report information on cloud backup

Use cloud backup information to monitor backup costs and help optimize your cloud backups.

Cloud backup information can be obtained from the following sources:

- [Cloud backup and recover reports on page 416](#)
- `mminfo` command
  - Use the `mminfo -avot` command to get information on how much data is consumed in a cloud backup.

## Cloud storage device staging

Staging with a cloud storage device works the same way as staging to a tape device. You cannot however, use a cloud storage device as the source for a staging operation. [Staging Backups on page 341](#) provides more information.

## Cloud storage device cloning

Cloning with a cloud storage device works the same way as cloning with any other advanced file type device. [Cloning on page 319](#) provides more information.

# CHAPTER 5

## Backup to Tape and VTL

This chapter contains the following topics:

• <a href="#">Overview of tape device storage</a> .....	180
• <a href="#">Stand-alone devices</a> .....	180
• <a href="#">SCSI data block size issues between UNIX and Windows</a> .....	181
• <a href="#">Device parameter settings</a> .....	183
• <a href="#">Setting the common device interface</a> .....	187
• <a href="#">Device ordering</a> .....	187
• <a href="#">Dynamic drive sharing</a> .....	191
• <a href="#">Deduplication rate improvements for Data Domain in VTL multiplexed backups</a> ..	197
• <a href="#">Nonrewinding tape device usage (UNIX/Linux only)</a> .....	199
• <a href="#">Support for LTO-4 hardware-based encryption</a> .....	200
• <a href="#">Whether to add or recycle volumes</a> .....	200
• <a href="#">Displaying device operations messages</a> .....	201
• <a href="#">Device Service mode</a> .....	201

## Overview of tape device storage

This chapter contains information on the creation, configuration, and management of tape devices. These may be configured as stand-alone devices or configured as part of a traditional tape library or virtual tape library (VTL) storage system.

The libraries and devices available to a NetWorker server are listed in the Devices view of the NetWorker Administrator window. The details and settings of a particular device can be viewed by right-clicking the device and selecting Properties. The full range of property attributes can be viewed by selecting View > Diagnostic Mode. A description of the various attributes is provided by the Field Help button.

As with other Console functions, you can view and work with only those NetWorker servers for which you have access permission.

## Stand-alone devices

A Device resource must be created for each stand-alone tape device on a storage node. Stand-alone drives must be configured individually.

Storage nodes must have been created before devices can be configured to be used by them. [Storage nodes on page 124](#) provides information about storage nodes and how to create them. Note that all scanning for devices is done at the storage node level, and can be done across multiple storage nodes. Only devices that have serial numbers can be autoconfigured. Use the `jbconfig` command to configure devices that do not have serial numbers.

---

### Note

Devices must be updated to the most recent firmware and drivers.

---

## Autodetecting and configuring a stand-alone tape drive

You can configure a new stand-alone tape drive, automatically by using Scan for Devices.

### Procedure

1. In the server's **NetWorker Administration interface**, click **Devices**.
2. Right-click **Devices** in the navigation tree, and select **Scan for Devices** to detect available devices. The **Scan for Devices** window appears.
3. Click **Start Scan**.
4. Check the scan status by clicking the **Monitoring** button and selecting the **Log** tab. Then return to the Devices navigation tree.
5. Select either the **Devices** folder or the **Storage Nodes** folder in the navigation tree. All detected drives are listed. Any still-unconfigured drives are preceded by a circular icon that displays a wrench.
6. Right-click the stand-alone drive to be configured, and select **Configure Drive**. A **Configuration** dialog box appears.
7. Click **Yes** to confirm that the drive should be configured. The new drive is automatically configured.

## Adding a stand-alone device manually

### Procedure

1. In the server's **NetWorker Administration** interface, click **Devices**.
2. Right-click **Devices** in the navigation tree, and select **New**. The **Create Device** window appears, with the **General** tab selected, and a default device path in the **Name** field of the **Identity** area of the window.
3. Replace the default name with the path and name of the device:
  - a. If the device is configured on the server's storage node, the name is the simple device path, such as /tmp/d0 for a file type device. A tape device on Microsoft Windows would have a format similar to \\.\Tape0.
  - b. If the device is configured on a remote storage node, however, then the name must indicate that the storage node is remote, by including rd= and the name of the remote storage node in the device path. For example, if the remote storage node is neptune, then the device path might be rd=neptune:/tmp/d0 or rd=neptune:\\.\Tape0.

[File type devices on page 156](#) provides instructions and restrictions on backing up to a file type device.
4. In the **Identity** area, configure:
  - a. In the **Comment** field add an optional, descriptive comment.
  - b. In the **Media Type** field, select a media type.
5. In the **Status** area, configure the applicable checkboxes:
  - **Read Only**
  - **Auto Media Management**
6. In the **Cleaning** area, configure the applicable fields:
  - **Cleaning Required**
  - **Cleaning Interval**

The Date Last Cleaned is filled in automatically once a drive has been cleaned.
7. Select the **Configuration** tab to set attributes, such as:
  - Target Sessions
  - Max Sessions
  - Local Backup to a dedicated storage node

NDMP settings (NDMP remote username and password are required for an NDMP device that acts as a storage node.)
8. Click **OK** when the configuration is complete.

## SCSI data block size issues between UNIX and Windows

Different SCSI hardware limitations exist between UNIX and Microsoft Windows operating systems. This can lead to data block size compatibility problems (although they are less likely to occur now than in the past, given larger Fibre-Channel capacities). For example, with a device defined in UNIX that is physically attached to a Windows HBA, it is possible to define a block size greater than that allowed by the Windows hardware. This could

lead to I/O errors in both write and read states on the device. In order to use both operating systems, it is necessary to determine a block size that is acceptable to both.

**NOTICE**

In NetWorker 8.0.1 and later, the default block size for an LTO device increases from 128 KB to 256 KB. When NetWorker labels a new or used volume in an LTO device and the Device block size attribute of the device is handler default, the label operation uses a 256 KB block size.

---

## Determining the allowable block size

You can determine the allowable block size by checking the Properties window of a mounted volume while in Diagnostic Mode.

**Procedure**

1. In the server's **NetWorker Administration interface**, click **Devices**.
2. Select **View > Diagnostic Mode**.
3. Open the **Libraries** folder in the navigation tree and select the drive that contains the mounted volume with the block size being checked. The drive's detail table appears.
4. Right-click the drive in the detail table, and select **Properties**. The **Properties** window appears.
5. Select the **Volume** tab. In the **Loaded Volume** area, one of the displayed volume attributes is the **Volume Block Size**.
6. Click **OK**.

## Solving block-size compatibility problems

---

**Note**

It is also possible to solve problems with block-size compatibility by changing the block size for an entire device type. The change, however, must be made on each storage node where it is to be available. Once the block size is changed, it affects only those volumes that are labeled after the change. Volumes can be relabeled to use the new block size, but if they contain data that should be saved, be sure to clone the data beforehand to a volume that already uses the new block size.

---

**Procedure**

1. In the server's **NetWorker Administration interface**, click **Devices**.
2. Select **View > Diagnostic Mode** on the menu bar.
3. Open the **Libraries** folder in the navigation tree and select the drive that contains the mounted volume with the block size being checked. The drive's detail table appears.
4. Right-click the drive in the detail table, and select **Properties**. The **Properties** window appears.
5. Select the **Advanced** tab. In the **Device Configuration** area, the currently configured **Device Block Size** value is displayed.
6. Select the appropriate **Device Block Size** value.
7. Click **OK**.

## Setting the block size for a device type

### Procedure

1. Change the block size:

- On UNIX, change the block size by setting this environment variable to the greatest common value for both systems. For example:

```
setenv NSR_DEV_BLOCK_SIZE_MEDIA_TYPE value
```

where:

- *MEDIA\_TYPE* is the backup device type available to the NetWorker server (also found in the Media Type attribute on the General tab of the device's properties). The media type syntax must be all uppercase, with underscores (\_) replacing blank spaces and hyphens. Therefore, a device displayed in the NetWorker software as "8mm Mammoth-2" would be listed as:  
8MM\_MAMMOTH\_2
- *value* must be a multiple of 32 KB, with a minimum value of 32 KB.
- On Microsoft Windows only, install a later model HBA, or upgrade to drivers that can support up to 128 KB blocks. Windows also accepts the same environment variable format as UNIX to set block size.

2. Restart the NetWorker server in order for changed environment variables to take effect.

## Device block size for read and write operations

The block size for a volume is defined during the label operation. The label operation uses the value defined in the Device block size attribute for the Device or the value defined by the appropriate block size environment variable.

The block size for both read and write operations uses the block size defined in the volume header during the label operation rather than the device block size.

## Block-size mode (UNIX/Linux only)

Ensure that the block size mode for tape devices that are used with NetWorker software is set to variable. Otherwise, data recovery might fail. The procedure for setting the device block size varies depending on the operating system.

The operating system's documentation provides information about setting the tape device block size in the operating system.

## Device parameter settings

Device parameter settings can be modified for the devices the NetWorker software uses in two ways:

- Individually, through the NetWorker Administration interface.
- Globally, for all devices through operating system environment variables. The adjustment of environment variables should only be done by users who know the server environment and performance tuning requirements. For example, an administrator who wants to fine-tune performance by changing a certain setting for all LTO devices on a particular NetWorker server.

The variables (and their equivalent names in the Administration interface) are described in these sections:

- [Setting device parameters in the NetWorker Administration interface on page 184](#)
- [Device setting environment variables on page 184](#)

## Setting device parameters in the NetWorker Administration interface

You can locate and change the device parameters in the Administration interface.

### Procedure

1. In the server's **Administration interface**, click **Devices**.
2. Select **View > Diagnostic Mode**.
3. Select **Devices** in the navigation tree. The Devices detail table appears.
4. Double-click the device in the devices table or right-click the device and select **Properties**. The Properties window appears, with the **General** tab selected.
5. Select the **Advanced** tab. In the **Device Configuration** area, the device settings are the first fields shown. The following table lists the fields and their corresponding environment variables:

### Results

**Table 27** Device settings and environment variables

Device setting	Corresponding environment variable
Device Block Size	NSR_DEV_BLOCK_SIZE_MEDIA_TYPE
Device File Size	NSR_DEV_TAPE_FILE_SIZE_MEDIA_TYPE
Device Load Time	NSR_DEV_LOAD_TIME_MEDIA_TYPE
Device Eject Time	None
Device Poll Interval	NSR_DEV_LOAD_POLL_INTERVAL_MEDIA_TYPE
Device Min Load Tries	NSR_DEV_LOAD_TRY_LIMIT_MEDIA_TYPE
Device Default Capacity	NSR_DEV_DEFAULT_CAPACITY_MEDIA_TYPE
Device Tape Flags	None

When device parameters are set in this interface, it is not necessary to stop and restart the NetWorker server in order for the settings to take effect.

## Device setting environment variables

There are several device-related environment variables available to configure devices for the NetWorker software.

Device-related environment variables include the following:

- NSR\_DEV\_BLOCK\_SIZE\_MEDIA\_TYPE
- NSR\_DEV\_TAPE\_FILE\_SIZE\_MEDIA\_TYPE
- NSR\_DEV\_LOAD\_TIME\_MEDIA\_TYPE
- NSR\_DEV\_LOAD\_POLL\_INTERVAL\_MEDIA\_TYPE
- NSR\_DEV\_LOAD\_TRY\_LIMIT\_MEDIA\_TYPE

- NSR\_DEV\_DEFAULT\_CAPACITY\_MEDIA\_TYPE  
where:

*MEDIA\_TYPE* is the backup device type available to the NetWorker server.

---

#### Note

The media type syntax must be all uppercase, with underscores (\_) replacing blank spaces and hyphens. For example, a device displayed in the NetWorker software as “8mm Mammoth-2” would be listed as: 8MM\_MAMMOTH\_2

To determine the media type, right-click the device and select the **General** tab. The **Media Type** attribute contains the media type that should be used in these environment variables.

---

## Setting device environment variables on Windows

Setting environment variables for the NetWorker software differs on Windows and UNIX operating systems.

Environment variables on Microsoft Windows are set using the Control Panel System applet on the NetWorker server.

#### Procedure

1. Navigate to Control Panel -> System and Security -> System -> Advanced System Settings.
2. In the General tab click Environment Variables...
3. Click the New button.
4. Specify the environment variable name and value.
5. Stop and start the NetWorker Backup and Recover Server service in order for the environment variables to take effect.

## Setting device environment variables on UNIX

Setting environment variables for the NetWorker software differs on Windows and UNIX operating systems.

NetWorker 8.0 introduces support for a new NetWorker environment variable file. This file, /nsr/nsrrc, will be sourced prior to starting the NetWorker processes.

#### Procedure

1. On the NetWorker server, modify the /nsr/nsrrc file. If this file does not exist, create this file as a Bourne shell script file.
2. Add the environment variables in the following format:

```
ENV_VAR_NAME = value
export ENV_VAR_NAME
```

3. Stop and start the NetWorker server processes in order for the environment variables to take effect.

## NSR\_DEV\_BLOCK\_SIZE\_MEDIA\_TYPE

NSR\_DEV\_BLOCK\_SIZE\_MEDIA\_TYPE is organized in units of kilobytes. This environment variable will cause NetWorker to override the default block-size setting defined for the tape drive in the operating system. The value set must be a multiple of 32, with a minimum value of 32. Maximums are determined by platform, SCSI driver, and device.

For example:

NSR\_DEV\_BLOCK\_SIZE\_4MM\_20GB=64

For information about using this environment variable to set block-size compatibility between UNIX and Microsoft Windows. [SCSI data block size issues between UNIX and Windows on page 181](#) provides more information.

## NSR\_DEV\_TAPE\_FILE\_SIZE\_MEDIA\_TYPE

NSR\_DEV\_TAPE\_FILE\_SIZE\_MEDIA\_TYPE is organized in units of NSR\_DEV\_BLOCK\_SIZE\_MEDIA\_TYPE and is the number of blocks written between filemarks. These filemarks are used to locate a particular spot on the tape during recovery, and more filemarks generally lead to faster positioning. For example:

NSR\_DEV\_TAPE\_FILE\_SIZE\_TZ89=512

On UNIX and Linux platforms, the NetWorker software writes a filemark by closing and reopening the tape device, which takes one or two seconds. If this value is too small, throughput could be slowed and recoveries may take longer to complete.

On Microsoft Windows platforms, the NetWorker software writes asynchronous filemarks. This setting has a minimal effect on performance.

## NSR\_DEV\_LOAD\_TIME\_MEDIA\_TYPE

NSR\_DEV\_LOAD\_TIME\_MEDIA\_TYPE is the number of seconds that nsrmmmd polls and waits for a drive to become ready after the library inserts a tape into the device.

NSR\_DEV\_LOAD\_POLL\_INTERVAL\_MEDIA\_TYPE is used to set the number of seconds nsrmmmd waits between polls during load time.

If the value of NSR\_DEV\_LOAD\_TIME\_MEDIA\_TYPE is too short, there could be unnecessary load failures. If it is too long, then labeling new tapes takes longer than necessary. The minimum allowable value is 10 seconds. The maximum value is 600 seconds. For example:

NSR\_DEV\_LOAD\_TIME\_DTL8000=300

## NSR\_DEV\_LOAD\_POLL\_INTERVAL\_MEDIA\_TYPE

NSR\_DEV\_LOAD\_POLL\_INTERVAL\_MEDIA\_TYPE is the number of seconds that nsrmmmd waits between each attempt to read a newly inserted tape. The minimum allowable value is 1 second, the maximum value is 30 seconds. For example:

NSR\_DEV\_LOAD\_POLL\_INTERVAL\_DLT=10

## NSR\_DEV\_LOAD\_TRY\_LIMIT\_MEDIA\_TYPE

NSR\_DEV\_LOAD\_TRY\_LIMIT\_MEDIA\_TYPE is the number of times that nsrmmmd will attempt to open a drive. The nsrmmmd program will poll the drive until the limit set in NSR\_DEV\_LOAD\_TIME\_MEDIA\_TYPE is reached. After the limit is reached, it will retry until the NSR\_DEV\_LOAD\_TRY\_LIMIT\_MEDIA\_TYPE is reached. The default value and minimum allowable value is 2, the maximum value is 120.

NSR\_DEV\_LOAD\_TRY\_LIMIT\_DLT=4

## NSR\_DEV\_DEFAULT\_CAPACITY\_MEDIA\_TYPE

NSR\_DEV\_DEFAULT\_CAPACITY\_MEDIA\_TYPE is the size of the particular tape used to base the percent full calculation. This variable value has no effect on the actual tape capacity. Any integer value is allowed, with a KB, MB or GB designation to indicate a range of values. Any value less than 200 MB will be overridden by the normal default capacity. There is no obvious maximum, with the only practical limitation being the actual storage size. For example:

NSR\_DEV\_DEFAULT\_CAPACITY\_DTL7000=12GB

## Setting the common device interface

The common device interface (CDI) allows the NetWorker server to send commands to tape devices. The CDI feature is not supported within an NDMP environment. CDI support can be set in the NetWorker Administration interface.

### Procedure

1. In the server's **NetWorker Administration interface**, click **Devices**.
  2. Select **View > Diagnostic Mode**.
  3. Select **Devices** in the navigation tree. The **Devices** detail table appears.
  4. Double-click a device in the **Devices** table (or right-click the device and select **Properties**). The **Properties** window appears, with the **General** tab selected.
  5. Select the **Advanced** tab. In the **Device Configuration** area, locate the CDI settings:
    - **Not Used:** Disables the CDI feature and uses standard tape driver calls for tape operations.
    - **SCSI Commands:** Sends explicit SCSI commands to tape devices.  
When enabled, the CDI feature:
      - Provides clearer tape status messages.
      - Informs when a tape is write protected.
      - Enables Tape Alert, which provides diagnostic information for devices.
- Although the CDI feature can be disabled through selecting the Not Used option, it can be time-consuming to disable a large number of devices.

In this situation, access the `/nsr/debug` directory and create a file named `cdisable`. Then restart the NetWorker server. This file does not need any content, it just needs to exist. This disables the use of CDI for that server and all storage nodes controlled by that server.

### Note

Use of CDI does not change what is written to tape. A tape written with CDI enabled can be read with CDI disabled. Conversely, a tape written with CDI disabled can be read with CDI enabled. The CDI feature enables NetWorker software to collect better diagnostic information and facilitates tape usage when enabled. Only set or disable the CDI feature on the advice of an EMC Customer Support representative. If tape or SCSI issues occur while the CDI feature is enabled, go to the EMC online support.

## Device ordering

The NetWorker server uses logical device names assigned by the operating system when communicating with devices. It is possible for the operating system to re-associate logical device names with the physical addresses of the devices, generally after rebooting the host or after plug-and-play events. This may cause device reordering, where the physical device will have a different device filename. As a result, tape devices configured in the NetWorker software no longer match the names of the devices as recognized by the operating system.

If device reordering occurs, the NetWorker software is unable to use any affected drives until the configuration is manually corrected.

The NetWorker server detects device reordering events by comparing the current serial number of the device to the serial number of the device at configuration. If the serial numbers do not match, the NetWorker server stops all operations on that device and an error message will be posted, similar to the alert identified for device serial number mismatch in the table [Preconfigured notifications on page 446](#). CDI must be enabled for this functionality. [Setting the common device interface on page 187](#) provides more information about enabling CDI.

## Persistent binding and naming

Some operating systems provide the persistent binding option to permanently bind logical and physical addressing so that the associations are retained. This guarantees that the operating system always uses and creates the same symbolic path for a device is known as persistent naming.

Proper configuration of the operating system to use persistent binding and persistent naming resolves issues related to device ordering by forcing the operating system to always assign the same device filename regardless of external events.

### Persistent binding

Persistent binding guarantees that the operating system always uses the same SCSI target ID for SAN devices, regardless of reboots or other events, by statically mapping a target's WWN address to a desired SCSI address. On some operating systems, this is done by default, while on others it has to be set manually. The operating system documentation provides further information.

In most cases, persistent binding should also be set on the Host Bus Adapter (HBA) by using the configuration utility that comes with the Fibre Channel HBA. The HBA device driver documentation provides details.

Persistent binding is required for consistent library operations within NetWorker, because the NetWorker server communicates with the library controller over a SCSI address that is chosen during initial library configuration. If the SCSI address changes, the library will become unavailable. In this case, disable the library and change the “control port” address to reflect the new SCSI address of the library controller.

If devices have already been configured in NetWorker prior to enabling persistent binding on the host, delete existing devices from the library resource and perform a re-scan of devices followed by a reconfiguration of the tape library.

### Persistent naming

Persistent naming is used to ensure that the operating system or device driver of a server always creates and uses the same symbolic path for a device (referred to as device file).

Once persistently named device files are created and present on the host, enable the use persistent names option when scanning for tape devices from the NetWorker Management Console.

If devices have already been configured in NetWorker prior to enabling persistent naming on the host, delete existing devices from the library resource and perform a re-scan of devices followed by a reconfiguration of the tape library.

## Detecting device ordering issues

To determine if there is a problem with device ordering in your environment, you first determine if the device order that appears in nsrjb output matches the device order from

the inquire and sjisn commands, then verify that the device configuration within your NetWorker configuration conforms to this.

#### Procedure

1. Execute the `inquire` command with the `-cl` option to determine the device path, scsi address, and serial number of the device.
2. Execute the `sjisn` command to determine the current order of the devices:

```
sjisn scsidesv@bus.target.lun
```

where bus.target.lun is the SCSI address of the robotic arm returned by the inquire command in step 1, for example, 1.2.0.

3. Match the serial numbers of the devices in the sjisn output to the device names that correspond to these serial numbers in the inquire `-cl` output. This will give you the current device order by device filename.
4. Execute the `nsrjb` command to determine the order of devices as configured in NetWorker. Drive entries towards the end of the nsrjb output list the device order as configured in NetWorker.
5. Compare the device ordering as determined in step 3 and step 4. If the device ordering in these two steps do not match, the device ordering has changed and the library will need to be reconfigured.

## Drive ordering change corrections

After a drive ordering change has taken place and the NetWorker software is no longer correctly communicating with devices, you can correct the problem within your NetWorker configuration by using the NetWorker Console or the jbedit command line program.

### Using NetWorker Console to correct drive ordering changes

You can correct drive ordering changes by using the NetWorker Console.

#### Procedure

1. Ensure that you have a current backup of the resource database.
2. Delete the library resource in the NetWorker Console. [Deleting libraries on page 145](#) provides details.
3. Rescan the library. [Scanning for libraries and devices on page 132](#) provides more information.

### Using the jbedit command to correct drive ordering changes

You can correct drive ordering changes by using the `jbedit` command.

#### Procedure

1. Use the `jbedit` command with the `-d` option to delete devices from the NetWorker configuration.
2. Use the `jbedit` command with the `-a` option to add the devices again.

[Library configuration using the jbedit command on page 137](#), or the UNIX man page for `jbedit` or the *EMC NetWorker Command Reference Guide* provides more information on the `jbedit` command.

## Clearing device ordering/serial mismatch errors from the NetWorker Console

After a device ordering error has been detected, a message is displayed in the Alerts and Notifications windows of the NetWorker Management Console, as well as the log files. The error message is similar to the following:

```
"Check system device ordering. Moving device on %s to . To correct, scan for devices in NMC and re-enable the device."
```

An Event ID for the error is also created, which will be removed along with the alert when the problem is resolved. You can resolve the problem and clear the error message.

### Procedure

1. Disable the drive.
2. Perform one of the above procedures to correct the problem.
3. Re-enable the drive, and retry the operation that was being performed prior to receiving the error.

### Results

The Alert will be removed and the event dismissed.

## Tape drive number reordering (Microsoft Windows only)

If more than one tape drive is attached to the NetWorker server when both the server and drives are shut down, restart all of the tape drives, either before or immediately after the NetWorker server is restarted. If Windows does not locate all of its previously configured tape drives at the time of startup, it automatically reassigns the tape registry name.

For example, assume that these three tape drives are attached to the server:

- The first one, \\.\Tape0, is a 4 mm tape drive.
- The second, \\.\Tape1, is an 8 mm tape drive.
- The third, \\.\Tape2, is also an 8 mm tape drive.

If only the second and third tape drives are restarted, Windows reassigns the tape registry numbers so that the second storage device becomes \\.\Tape0 and the third storage device becomes \\.\Tape1. The tape registry numbers no longer match the defined storage devices within the NetWorker software. As a result, the server mishandles the drives and their volumes.

It might be easier to leave a nonoperational drive (device) attached to the server until a replacement is available. If the drive is removed, the name must be deleted, and then the new drive must be added.

To disable the drive, select No for the Enabled attribute in the device's Properties.

## Device calibration

For information about the frequency and method for calibrating the loading mechanism for the device, refer to the library manufacturer's documentation.

# Dynamic drive sharing

Dynamic Drive Sharing (DDS) is a feature that provides NetWorker software with the ability to recognize shared physical tape drives. DDS enables NetWorker software to do the following:

- Skip the shared tape drives that are in use.
- Route the backups or recoveries to other available shared tape drives.

## Introduction to DDS

DDS controls application requests for tape media and allows the NetWorker server and all storage nodes to access and share all attached devices.

A system administrator can configure DDS by setting a sharing policy for devices that are accessible from multiple storage nodes.

Two terms central to the use of DDS are drive and device. Within the context of DDS, these terms are defined as follows:

- Drive — The physical backup object, such as a tape drive, disk, or file.
- Device — The access path to the physical drive.

**NOTICE**

DDS is currently supported only in a storage area network (SAN) Fibre Channel environment and not in a direct-connect SCSI environment.

## Benefits of DDS

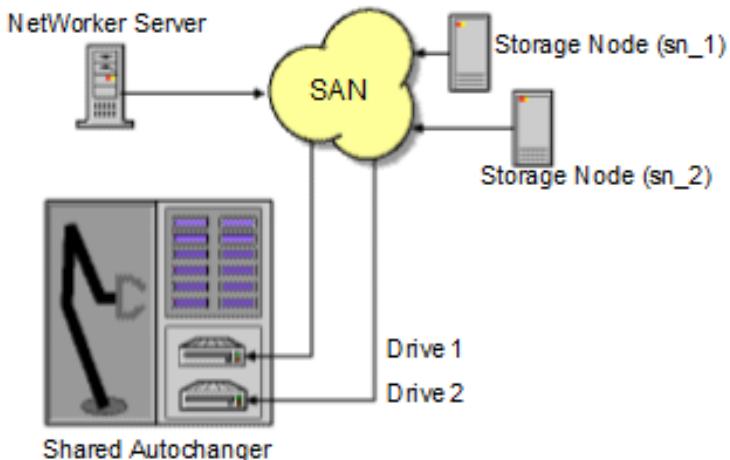
Enabling DDS on a NetWorker system provides these benefits:

- Reduces storage costs — A single tape drive can be shared among several storage nodes. In fact, since NetWorker software uses the same open tape format for UNIX, Windows, NetWare and Linux, the same tape can be shared between different platforms (assuming that respective save sets belong to the same pool).
- Reduces LAN traffic — Clients can be configured as SAN storage nodes that can send save sets over the SAN to shared drives.
- Provides fault tolerance — Within a SAN environment, hardware can be configured to eliminate a single point of failure.
- Provides configuration over a greater distance — Allows configuration of a system over a greater distance than with SCSI connections.

## DDS configuration overview

The following figure illustrates the DDS process and potential configurations for sharing drives. This basic configuration consists of a server, two storage nodes, and a library with two tape drives.

**Figure 11** Dynamic Drive Sharing



In this figure:

- Storage nodes sn\_1 and sn\_2 are attached to the library.
- Each node, on its own, has access to drive\_1 and drive\_2.
- With DDS enabled, both nodes have access to both drives and can recognize when a shared drive is in use.

Under such a configuration, two DDS licenses are required, one for each drive.

**NOTICE**

---

Ensure that all applicable devices can be seen from each storage node by running the inquire -l command locally on each storage node.

## DDS block-size compatibility between UNIX and Windows

With DDS enabled, drives can be shared between storage nodes on different platforms, such as UNIX and Microsoft Windows. For NetWorker software operations (such as backups and recoveries) to take place successfully, ensure that the block size is compatible between different platforms and/or hardware.

To ensure compatibility, make sure one of the following conditions is met:

- The various storage nodes sharing a drive support the same block sizes.
- When a tape is labeled on a drive, it is labeled with the block size defined on the storage nodes.

[SCSI data block size issues between UNIX and Windows on page 181](#) provides information about how to set block sizes for individual drives or tapes on different platforms.

## Block-size incompatibility between UNIX and Windows

Incompatible block-size settings between UNIX and Microsoft Windows storage nodes could result in any of these error scenarios:

- A backup taken on a UNIX node might not be recoverable on a Microsoft Windows node if the Windows node does not support large block sizes.
- A UNIX process labels and saves data to a tape and leaves the tape mounted. A Microsoft Windows process subsequently attempts to verify the label on this tape and fails because the label verification is done by reading a header from the data portion.
- A tape on a UNIX node is labeled with a large block size. The backup is started on a Microsoft Windows node and the Windows node attempts to write the backup by using the default block size. Internally, the backup on Windows is written by breaking down the big buffer of data into smaller segments of writable block sizes. Attempting to recover a specific file on Windows in this situation fails due to positioning errors on the tape. The data is still recoverable from the Windows side, since the NetWorker software will switch from using file and block positioning to reading the tape from the beginning to reach the correct position. The data might not, however, be recoverable from the UNIX side.

## Unintended Access to DDS device prevention

The Reserve/Release attribute has been added to the Device resource for tape devices to support Reserve/Release, including the Persistent Reserve commands.

Reserve/Release is a mechanism that uses SCSI commands to attempt to prevent unintended access to tape drives that are connected by using a shared-access technology, such as Fibre Channel, iSCSI, or SCSI multiplexers. It is a “cooperative” and host-based mechanism, which means that all applications should respect the reservations and not purposely break them. Access is granted based on the host system that reserved the device. Other applications that run on that host cannot be prevented from accessing a reserved device.

Reserve/Release cannot prevent a malicious or badly behaved application from accessing a reserved device. It also cannot prevent all problems caused by hardware issues (such as SCSI resets or FC LIPs) from interrupting data access.

The basic sequence requires that a host reserve a tape drive (using specific SCSI commands) before attempting to access the tape drive. If this “reservation” succeeds, then the host can use the drive. If the reservation fails (usually because the device is reserved by someone else), then the host attempting the reservation should not attempt to use the drive. When a host has finished using a reserved drive, that host must release the drive by using the appropriate SCSI commands.

The reservation is maintained by the drive itself. With older (called “Simple” in NetWorker software) Reserve/Release, the reservation is based on the SCSI ID of the system that issued the reserve command. For tape drives connected to Fibre Channel (FC) using FC-SCSI bridges, the mapping between FC host and reservation is done inside the bridge, since the initiator on the SCSI side is always the bridge itself, regardless which host actually issued the reserve command.

For Persistent Reserve, the reservation is associated with a 64-bit “key” that is registered by the host. Several keys can be registered with a given drive at any given time, but only one may hold the active reservation. NetWorker software uses the “exclusive” reservation method for Persistent Reserve. Only the host that holds the active reservation is allowed to access the drive.

The Reserve/Release attribute does not support file type or advanced file type devices.

The settings that relate to Reserve/Release and Persistent Reserve are found in a device's Properties window, on the Advanced tab. They are visible only when diagnostic mode is turned on.

The default setting for Reserve/Release is None. Once any other Reserve/Release setting is selected, it works automatically, without further user intervention. The Reserve/Release attribute is supported only on Common Device Interface (CDI) platforms, so if the CDI attribute in a device's Properties is set to Not Used, then Reserve/Release settings are ignored. [Setting the common device interface on page 187](#) provides more information regarding CDI.

For newer hardware, once a Reserve/Release setting (other than None) has been selected, the appropriate Persistent Reserve commands are automatically issued before a device is opened for reading or writing, and before the device is closed. With older hardware, a SCSI-2 Reserve command is issued before opening the device, and a SCSI-2 Release command is issued after the device is closed.

Reserve/Release has these possible settings:

- None (the default)
- Simple
- Persistent Reserve
- Persistent Reserve + APTPL (Activate Persist Through Power Loss)

The Persistent Reserve Key attribute has also been added. It is used with Persistent Reservation calls.

## Restrictions for use of the SCSI Reserve/Release setting

There are restrictions for using the SCSI Reserve or Release setting.

Consider the following:

- It is available on CDI platforms only. Consequently, since CDI is not supported within an NDMP environment, Reserve/Release is not supported with NDMP.
- Not all drives support persistent Reserve/Release. (All drives support at least simple reserve release. The code automatically drops back from Persistent +APTPL or Persistent to Simple on drives that do not support Persistent.)
- SCSI resets can clear Simple reservations at the device.
- Even with Reserve/Release, there is no guarantee against data loss.
- If the operating system has its own Reserve/Release feature, that feature must be disabled in order for the NetWorker Reserve/Release feature to work.
- Even if all of the enterprise's NetWorker storage nodes have this feature enabled, then it is possible that, on the storage node where a backup operation is run, data loss can be caused by the operating system's utilities or by third-party programs.

## DDS on NDMP nodes in a SAN environment

Drives can be shared between NDMP nodes in a SAN environment.

Consider the following:

- All the components of a SAN configuration must be compatible when DDS is enabled with the NetWorker NDMP feature.
- The Fibre Channel switches must be compatible with any NDMP hosts within a SAN.
- NDMP hosts and libraries in the SAN must also be compatible with each other.
- The NDMP nodes that will share the drives are homogeneous. For example, DDS can be enabled in these configurations:

- EMC Celerra® to EMC Celerra
- NetApp to NetApp (any NetApp nodes that Network Appliance supports within a zone)
 

The current NDMP implementation does not allow the sharing of drives between non-homogeneous NDMP nodes. There is, however, no inherent limitation within DDS that would prevent this.

## NetApp zoning requirements for DDS in a SAN environment

To configure DDS with NetApp filers, a zoned SAN configuration is required. Zoning is a feature of the Fibre Channel switch.

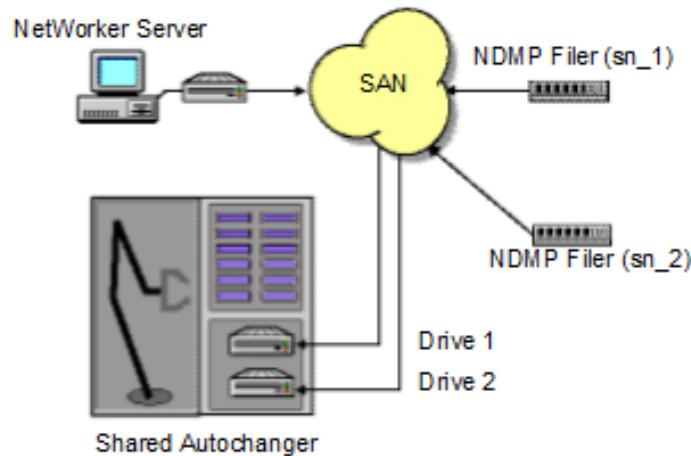
Consider the following when configuring DDS with NetApp filers:

- The NetApp zone, which contains only the NetApp filers and tape devices, must be configured on the Fibre Channel switch. This NetApp zone may also include the robotic arm and must also be configured in an arbitrated loop.
- All non-NetApp servers that are attached to the same Fibre Channel switch must be excluded from the NetApp zone. A separate zone must be configured for the non-NetApp servers, in which an arbitrated loop may or may not be a requirement.
- The NetApp zone and all other zones can overlap on the tape devices within the SAN, so that the tape devices are visible to both zones.

This figure illustrates a basic DDS configuration with NDMP:

- Both the NDMP Filer (sn\_1) node and the NDMP Filer (sn\_2) node must be the same kind for DDS to be enabled.
- The hardware id for Drive 1 is drive\_1
- The hardware id for Drive 2 is drive\_2.
- 

**Figure 12** DDS with NDMP



## DDS attributes in the device properties

Configure the attributes used in DDS from the Properties window for a device.

The attributes include:

- Hardware ID

- Shared Devices

## Hardware ID attribute

The Hardware ID attribute tracks the drives that are being shared by multiple hosts. Device instances sharing the same physical drive across multiple hosts have the same hardware ID. The hardware ID is automatically assigned during the device autoconfiguration process, or it can be added when manually configuring a device. It is not editable by users.

The hardware ID can be viewed in the Properties window for a device, on the General tab, in the Device Sharing area.

The hardware ID is generated when a device is scanned or configured. The hardware ID consists of the following:

- The hardware serial number
- The device type
- The worldwide part number (WWPN)
- The worldwide name (WWN)

Do not try to change a hardware ID once it has been generated. It is read-only.

## Shared Devices attribute

The Shared Devices attribute appears on the Operations tab of a device's Properties when in diagnostic mode. It features values that can be used to manipulate all shared instances of a drive at the same time. This attribute enables or disables all devices that share the same hardware ID with a single action. The following table lists this attribute's allowed values and their descriptions.

**Table 28** Shared Devices attributes

Value	Description
Enable All	When selected, enables all devices by using the same hardware ID.
Disable All	When selected, disables all the devices by using the same hardware ID.
Done	This is the default setting. After the server has enabled or disabled all devices with the same hardware ID, the attribute is reset to Done.

The Shared Devices attribute is not reflected in the jbconfig program.

## Idle Device Timeout attribute and DDS

A tape might remain mounted in its drive after a backup has completed. Other requests for the drive from another device path must wait during this timeout period. The timeout value can be adjusted by changing the Idle Device Timeout attribute.

The Idle Device Timeout is not specifically a DDS attribute, but it can be useful in configuring shared drives. This attribute appears on the device Properties Advanced tab when displayed in diagnostic mode. The default value is 0 (zero) minutes, which means that the device never times out and the tape must be ejected manually.

If the device belongs to a library, you can also specify the Idle Device Timeout value for all devices in the library. However, the library's value will take effect only on those devices whose Idle Device Timeout value is 0. The library's Idle Device Timeout value is located on the Timer tab of the library Properties window. [Unmounting volumes automatically \(idle device timeout\) on page 217](#) provides more information.

## High availability and DDS

The NetWorker software relocates and restarts operations that were in progress when a failure occurs on a cluster node. Currently, savegroups are the only highly available operations.

### The nsrjb program high availability limitations

If the NetWorker server fails over from one node to a new target node, standard library operations (such as performing an inventory, labeling, mounting, or unmounting a volume) do not automatically restart on the new target node.

Example: Host crash requires user intervention

This example scenario includes: two physical hosts, A and B, with DDS enabled, sharing the drives on a library.

Physical host A mounts a tape in a shared drive on the library. If physical host A subsequently crashes, the volume is held in that shared drive until the reset command `nsrjb -H` is issued (from host B, in this example) along with a reset from the Library Operations Windows in the NetWorker Console.

This command unloads the drive and makes it available for future backups. The reset command clears the drive by accessing the device through another shared path. In this example, the other shared path would be on host B.

Successfully unloading a volume requires that the NetWorker software be able to access the same path through which the volume was initially loaded.

## Deduplication rate improvements for Data Domain in VTL multiplexed backups

New functionality has been introduced to improve tape deduplication ratios of multiplexed backups for remote client save streams. This pertains to non-dedicated storage nodes that use DD5.x VTL devices. With this functionality, significantly higher NetWorker de-duplication ratios are obtained without noticeable impact to the device MB/s throughput.

No special configuration is required when using a NetWorker dedicated storage node (DSN) or NetWorker saves directed to a local device.

To obtain the best deduplication rates, you would generally disable multiplexed deduplication by setting each VTL device's properties target sessions and max sessions values to 1. However, for environments with high overall concurrency requirements (for example, a large number of parallel backups required due to a limited backup window duration business requirement), an excessive number of virtual tape drives might not be possible, or might be in use but causing backup runtime stability problems, such as intermittent volume mount operation delays or timeouts. In this case, consider applying the new functionality, with slight increases to the max sessions, target sessions and device block size values and using a fraction of the previous number of VTL devices.

---

**Note**

When the new functionality is first enabled with the recommended increases in device block size and max sessions, backups will initially have lower deduplication ratios prior to achieving the higher target deduplication rate. This also occurs without the new functionality enabled, such as when switching from multiplexed to non-multiplexed backups, and reflects initial DDR re-priming or re-analysis overhead. Therefore, extra caution should be observed on DDR systems which are already heavily utilized (for example, 75% or more DDR disk space already used).

---

## Enabling the new functionality for network saves globally

Note that deduplication efficiency is still relative to the number of multiplexed save sets, and the ratio drops with higher concurrency. From measured tests, expected efficiency dropped by 4% to 8% for each additional parallel save stream.

For example, using a sufficiently large device block size and 4 parallel streams (where device property max sessions is set to 4), expected de-duplication ratios are 12-24% below the ideal (a non-multiplexed backup where max sessions is set to 1).

Additionally, the following best practices are recommended:

- Install DD OS version 5.0.2 or later if currently using DD OS 5.0.x. This version of DD OS addresses a large number of DD VTL specific issues, and has higher deduplication ratios in general than DD OS 4.9 versions for DD VTL use cases.  
If using DD OS 4.x, install DD OS version 4.9.3.1.
- The recommended block size is 512 KB. The standard NetWorker default block size (handler default) depends on the device type and varies between 32KB and 128KB. From measured tests, increased block size had an additional positive impact on deduplication efficiency of 15% to 25%.
- Adjust the number of VTL devices to a lower value to correspond to the new max sessions value. If considering the recommended values in step 2, the number of VTL devices can be inversely reduced: increase each device max sessions from 1 to 4, then decrease the number of required VTL devices to  $\frac{1}{4}$  of the current number.
- Change the device parameters for max sessions and device block size until a combination is obtained that results in higher deduplication ratios, a smaller backup window and increased system stability. Recommended values are provided in step 2.
- As a general best practice when performing deduplication, ensure that no client/server side encryption or compression occurs prior to reaching the Data Domain device.

More information is provided in the “NetWorker Improved Deduplication with Multiplexing to Data Domain VTLs” technical note available on the EMC Online Support website at [https://support.emc.com/docu37676\\_NetWorker-7.6.3-\(and-Later\)-Improved-Deduplication-with-Multiplexing-to-Data-Domain-VTLs.pdf](https://support.emc.com/docu37676_NetWorker-7.6.3-(and-Later)-Improved-Deduplication-with-Multiplexing-to-Data-Domain-VTLs.pdf)

### Procedure

1. Shut down the relevant NetWorker storage node's service (or the entire Networker server if possible).
2. After verifying there is no backup activity on the NetWorker DD VTL storage node, change the **max sessions** value for each relevant VTL device to 4 (recommended) up to 32 (maximum) using NMC or nsradmin. **Target sessions** and **device block size** should also be set accordingly.

Recommended values are max sessions = 4, target sessions = 4, and device block size = 512KB. However, the optimal values will depend on your environment (for

example, max sessions = 2 may provide better deduplication while still meeting your backup window without stability problems).

The following example provides a way to set the recommended values using the UNIX/Linux or Windows command line.

Run the following:

```
> nsradmin -i input_file.txt
```

where input\_file.txt contains the following example lines to be customized for your own environment:

```
> option regexp: on
> . type: nsr device; media type: LTO Ultrium-3; media family:
tape; name: /dev/rmt*
> update max sessions:4; target sessions: 4; device block size:
512kB
```

#### Note

If the NetWorker server was shut down in step 1, run this nsradmin command with the **-d resdir** option, which uses the NetWorker resource database resdir instead of opening a network connection.

3. Create a no-intra-block-multi-plexing (nibmp) tag file in the NetWorker debug folder on the NetWorker storage node. For example, using the standard NetWorker installation paths:

On Unix/Linux:

```
#touch /nsr/debug/nibmp
```

On Windows:

```
> echo > "<NetWorker_install_path>\nsr\debug\nibmp"
```

You can limit the patch to specific pools by adding \_<Pool name> to the end of the tag file. For example, if the pool name was My Pool:

On Unix/Linux:

```
#touch "/nsr/debug/nibmp_My_Pool"
```

On Windows:

```
> echo > "<NetWorker_install_path>\nsr\debug\nibmp_My_Pool"
```

The pool name can include spaces. Ensure there are quotes around the specified pathname.

4. Restart the NetWorker services to enable the functionality.

## Nonrewinding tape device usage (UNIX/Linux only)

Tape drives used as storage devices must be accessed by nonrewinding device files. The NetWorker server assumes that a tape is in the same position in which it was the last time it was accessed. If the operating system's device driver rewinds the tape, then the position is lost, and previously written data will be overwritten by the next backup.

The NetWorker configuration software automatically chooses the correct device pathname for tape devices. If the user specifies the pathname, then it must be

nonrewinding, and it must follow the Berkeley Software Distribution (BSD) semantic rules.

For example, /dev/rmt/0mbn, where:

- The b satisfies the BSD semantics requirement on Solaris and HP-UX.
- The n specifies nonrewinding behavior on Solaris, HP-UX, Linux, and HP-Tru64.

On AIX, the number following the decimal selects the BSD and nonrewinding behavior and must be either 1 or 5 for NetWorker software (for example /dev/rmt2.1)

---

#### Note

Never change a device pathname from nonrewinding (/dev/rmt/0cbn) to rewinding (/dev/rmt/0cb). When the pathname is changed to rewinding, the data could only be saved, but never recovered. All but the last save are overwritten by later saves.

---

## Support for LTO-4 hardware-based encryption

The use of LTO-4 hardware-based encryption is supported by NetWorker when controlled by management utilities that are provided with the LTO-4 hardware, or by third-party key management software. EMC does not test or certify these key management utilities; however, the NetWorker application can read from and write to LTO-4 devices that use hardware-based encryption. The use of this encryption is transparent to NetWorker. Neither the encryption nor the key management process is managed by the NetWorker application. This includes the ability to turn encryption on or off within NetWorker, and the management of encryption keys.

## Whether to add or recycle volumes

The NetWorker server saves files on volumes marked appen (appendable). If the volumes are marked full, they cannot receive backups. There are situations best suited to either adding a new volume, or recycling an existing volume.

If volumes are marked full, you can:

- Remove the full volumes and replace them with new media if the volumes are being kept for long-term storage.
- Change the volume mode to recyc (recyclable) if the data on the full volumes is not needed. The NetWorker server overwrites the data with new backups, but maintains the existing labels. [Changing a volume's mode on page 209](#) provides information about changing the volume mode.

When all of the save sets on the volume have passed the time period specified by the retention policy, the mode of the volume automatically changes to recyclable.

There are advantages both to recycling media and adding more media to a pool. With recycling, the same volumes are used repeatedly, and there is no need to add new volumes to the pool. The volumes can, however, wear out over time and exhibit a higher failure rate.

On the other hand, if backups are to be stored for some time, then it might be necessary to add more media to the pool instead of recycling. For example, a library might need new volumes every three months if the company policy is to maintain the backups for a year. In this case, new media must be added to the pool until the volumes that contain expired or old backups can be recycled.

# Displaying device operations messages

## Procedure

1. In the NetWorker Administration window, click **Monitoring**.
2. Select the **Operations** tab.
3. Right-click an operation, and select **Show Details**.  
The details window for the selected device appears.
4. Click **Close** to exit the window, or **Save** to save the message.

# Device Service mode

Use the service mode setting to take a device offline temporarily. Service mode differs from the disabled state in that the nsrmm process is not stopped.

While a device is in service mode, save or recover sessions that are either in process or pending are completed. No new sessions are assigned to the device while it is in service mode.

Although a drive in service mode is taken out of the collection of drives that the NetWorker software can select for automated operations, the drive is available for some manual operations that use the nsrjb or nsrmm command with the -f option. For more information, refer to the *EMC NetWorker Command Reference Guide* or the UNIX man pages.

The device might also go into service mode, rather than become disabled, if consecutive errors occur in excess of the maximum consecutive error count specified for the device. This means that if there are no hardware issues, the tape can be ejected and used in other drives. [Media handling errors on page 222](#) provides more information about how to set the maximum consecutive error count.

---

## Note

The drive must be manually reset to Enabled for the NetWorker software to use the device again.

---

# Setting the Service mode for a device

## Procedure

1. Open the device's **Properties** window.
2. On the **General** tab, set **Status Enabled** to **Service**.



# CHAPTER 6

## Media Management

This chapter contains the following topics:

- [Storage management operations](#).....204
- [Auto Media Management](#).....206
- [Volume operations](#).....207
- [Media handling errors](#).....222
- [Media management in a silo](#).....223
- [Volume save sets](#).....227

# Storage management operations

This section describes the components involved in the operation of storage volumes done through the NetWorker server. The details that describe a particular volume can be viewed, and often changed, by right-clicking the volume and making a selection from the menu. As with other Console functions, users can view and work with only those NetWorker servers for which they have access permission.

## How the NetWorker server uses volume labels

A volume label is a unique internal code, applied by the NetWorker server, that initializes the volume for the server to use and identifies a storage volume as part of a specific pool. [Using media pools on page 284](#) provides more information about pools. Labeling a volume provides a unique name for tracking and recognizing the media, as well as references to volume labels in the records stored in the media database. The NetWorker server uses the media database records to determine which volumes are needed for backing up or recovering data.

When it labels a volume, the NetWorker server:

1. Verifies that the volume is unlabeled.
2. Labels the volume with the name specified in the **Volume Name** attribute by using one of the following:
  - The next sequential label from the label template that is associated with the chosen pool.  
If a recyclable volume from the same pool is relabeled, the volume label name and sequence number remain the same, but access to the original data on the volume is destroyed. The volume becomes available for new data.
  - An override volume name that was entered by the user.

## Selecting a volume for the NetWorker server

When a backup takes place, the NetWorker server searches for a volume from the appropriate pool to accept the data for backup.

The available volumes are as follows:

- Mounted on stand-alone devices.
- Available for labeling and accessible to the NetWorker server through Auto Media Management or a library.
- Labeled for the appropriate pool and already mounted in a device, or are available for mounting, if a library is being used.

If two or more volumes from the appropriate pool are available, the server uses this hierarchy to select a volume:

### Procedure

1. Mounted volumes from the appropriate pool with the mode appendable are selected. This includes newly labeled volumes. If more than one mounted volume is appendable, the server uses this hierarchy:
  - a. Device availability. The server writes to the volume from the appropriate pool that is mounted on the device with the fewest current sessions.
  - b. Volume label time. The server writes to the volume with the oldest label time if the mounted volumes are appendable and session availability is not an issue.

2. If a library is in use and there is no mounted, appendable volume in the library, the server determines whether there is an unmounted, appendable volume available. This includes newly labeled volumes.
3. If multiple unmounted, appendable volumes are available, the volume with the oldest label time is selected.
4. If no mounted volumes are appendable and Auto Media Management is enabled, a mounted volume with the mode recyclable is selected. The server relabels and mounts the volume.
5. If a stand-alone device is being used and Auto Media Management is not enabled, the server sends a mount request notification.
6. If a library is in use and no unmounted, appendable volumes exist, the server determines whether there is an unmounted, recyclable volume.
7. If Auto Media Management is not enabled, or if there are no appendable or recyclable volumes, the server sends a mount request notification.

[Volume operations on page 207](#) provides information about appendable and recyclable volumes.

## Data recovery and volume selection

The NetWorker server determines which volumes are required for recovery. If the appropriate volume is currently mounted, the recovery begins. If the volume is not mounted and a library is used, the server attempts to locate and mount the volume in an eligible device for appropriate media pool. Preference is given to mount the volume in a read-only device, if one is available.

If a stand-alone device is used, or if the server cannot locate and mount the volume, the server sends a mount request notification.

If more than one volume is needed to recover the data, the NetWorker server displays all the volumes, in the order needed. During the recovery process, the server requests the volumes, one at a time.

### NOTICE

NetWorker will automatically unload volumes that have been placed in a jukebox device but have never been mounted (for example, nsrjb -l -n <volume>). Any command, such as the scanner command, that operates on volumes that have never been mounted will be affected by this behavior. To prevent NetWorker from unloading the volume, the device should be set to service mode while the command is being run.

## Automatic volume relabel

The NetWorker 8.0 and later software releases provide the ability to automatically relabel recyclable volumes when needed or when scheduled.

Consider the following:

- If Auto Media Management is enabled and a volume has the mode recyclable, the server automatically relabels the volume. A volume is automatically set to recyclable when all save sets on the volume, including partial save sets that span other volumes, are marked as recyclable. [Auto Media Management on page 206](#) provides more information on Auto Media Management.
- A media pool can be configured to automatically relabel recyclable volume at a user defined time and interval. [Managing volumes in a media pool on page 292](#) provides more information about configuring the automatic relabel process for recyclable volumes in a media pool.

- The mode of a volume can also be manually changed to recyclable. [Changing a volume's mode on page 209](#) provides information about changing the mode of a volume.

## Auto Media Management

Auto Media Management gives the NetWorker server automatic control over media loaded in the storage device.

When Auto Media Management is enabled during device configuration, the NetWorker server automatically:

- Labels the volume (recognizes EDM labels and does not overwrite them).
- Mounts the volume.
- Overwrites volumes it considers to be unlabeled.  
The NetWorker server considers a volume to be unlabeled under the following conditions:
  - Has no internal label.
  - Is labeled with information other than a NetWorker label.
  - Is labeled with a NetWorker label, but the density indicated on the internal label differs from that of the device where the volume is mounted.
- Recycles volumes eligible for reuse that are loaded into the device.
- Because the Auto Media Management feature can relabel a volume that has a different density, it is possible, inadvertently, to overwrite data that still has value. For this reason, be careful if NetWorker volumes are shared among devices with different densities.
- When the Auto Media Management feature is not enabled, the NetWorker server ignores unlabeled volumes and does not consider them for backup.

**NOTICE**

The NetWorker server considers volumes that were labeled by a different application to be valid relabel candidates if Auto Media Management is enabled. Once the NetWorker server relabels the volume, the previously stored data is lost.

## Existing tapes with NetWorker labels

When Auto Media Management is used with tapes that have NetWorker labels that have not been recycled, the volumes must be removed from the media database before a utility such as tar is used to overwrite the labels. Also ensure that the tapes have been fully rewound before overwriting the labels. Auto Media Management can then properly relabel the tapes.

## Auto Media Management for stand-alone devices

The Auto Media Management feature can be enabled for stand-alone devices during manual device configuration, or from the Properties window after configuration.

When Auto Media Management is enabled for a stand-alone device, the following processes occur when a volume becomes full during a backup:

- A notification is sent that indicates that the server or storage node is waiting for a writable volume. Simultaneously, the NetWorker server waits for the full, verified volume to be unmounted.

- The device is monitored and the software waits for another volume to be inserted into the device.
- After a volume is detected, a check is performed to determine whether the volume is labeled. If so:
  - The volume is mounted into the device.
  - The NetWorker server checks to see whether the newly mounted volume is a candidate to receive data:
    1. If yes, the write operation continues.
    2. If no, the NetWorker server continues to wait for a writable volume to continue the backup.
- If the volume is recyclable and is a member of the required pool, it is recycled the next time a writable volume is needed.
- If the volume is unlabeled, it is labeled when the next writable volume is needed for a save.

**NOTICE**

If a partially full volume is unmounted, the NetWorker server automatically ejects the volume after a few seconds. If a stand-alone device is shared between storage nodes, then Auto Media Management should not be enabled for more than one instance of the device. Enabling Auto Media Management for more than one instance of the stand-alone device will tie up the device indefinitely. No data is sent to the device and no pending message is sent.

---

## Enabling Auto Media Management for libraries

Auto Media Management is not enabled for libraries during autoconfiguration. Auto Media Management for a library can be set by changing the library's properties after configuration.

### Procedure

1. In the server's **Administration** window, click **Devices**.
2. Select the **Libraries** folder in the navigation tree. The Libraries detail table appears.
3. Right-click the library, and select **Properties**. The **Properties** window appears.
4. Select the **Configuration** tab.
5. In the **Media Management** area, select **Auto Media Management**.
6. Click **OK**.

## Volume operations

The volume operations sections describe the tasks involved in the operation of storage volumes done through the NetWorker server. Information about storage volumes is available for each device on a NetWorker server. All volume operations are performed in the Media task in the Administration window.

If a volume is not mounted when a backup is initiated, then one of three messages appears, suggesting that one of these tasks be performed:

- Mount a volume.
- Relabel a volume (only when Auto Media Management is enabled).
- Label a new volume (only when Auto Media Management is enabled).

During file recovery, the NetWorker server requests the volume name. If more than one volume is needed to recover the files, the server lists all the volumes in the order in which they are needed. During the recovery process, the server requests each volume, one at a time. If a library is used, the server automatically mounts volumes stored in the library.

The NetWorker server reports on the status of volumes using values such as:

- Volume name
- Written
- %Used
- Location
- Mode

Performing volume operations requires that the user have the correct permissions to use the NetWorker server and its storage nodes.

## Viewing volume status information

**Table 29** Volumes detail

Category	Description
Volume Name	Within the Administration interface, the volume name is the same as the name that appears on the volume label. At the end of the name, these designations might appear: (A) indicates an archive volume. (R) indicates a volume that is considered read-only. (W) indicates that the volume is a write once, read many (WORM) device.
Barcode	Barcode label, if one exists.
Used	Indicates the amount of space currently in use on the volume (shown in KB, MB, GB, as appropriate). When Used is equal to full, there is no more space on the volume and the end-of-tape marker has been reached or an error with the volume has occurred.
% Used	An estimate of the percentage used, based on the total capacity of the volume, and on the specified value of the Media Type of the Device resource. When %Used is equal to 100%, it means that the value is equal to, or exceeds, the estimate for this volume. When the word "Full" appears in the % Used column, it is not based on an estimate of the volume's capacity. "Full" literally means that the volume is full. This attribute applies only to tape volumes. File type and advanced file type devices always display 0% Used.
Mode	Choices are appendable, read-only, and recyclable. <a href="#">Changing a volume's mode on page 209</a> provides information on changing volume modes.
Expiration	Changing the expiration date is only possible from the command prompt. Use the nsrmm command to do this.
Location	Refers to an administrator-defined description of a physical location of the volume within the user's environment, for example, 2nd shelf, Cabinet 2, Room 42.
Pool	Name of the pool to which the volume belongs.

**Table 30** Volume modes

Mode value	Meaning	Description
appen	appendable	This volume contains empty space. Data that meets the acceptance criteria for the pool to which this volume belongs can be appended.
man	manual recycle	This volume is exempt from automatic recycling. The mode can be changed only manually. The manual recycle mode and the option to change it are available from the Volumes menu. The default recycle mode is Auto.
(R)	read-only	The save sets on this volume are considered read-only. The mode can be changed only manually. <a href="#">Read-only mode on page 209</a> provides more information.
recyc	recyclable	The save sets on this volume have exceeded their retention policies.
full	full	The volume is full. There is no more space for data in the volume, and the save sets have not yet passed the time periods specified by the retention policies. This mode can be set only from the command-prompt. Use the nsrb command with the -o option for libraries, and the nsrmm command with the -o option for stand-alone drives. Refer to the respective UNIX man pages of those commands (or to the <i>EMC NetWorker Command Reference Guide</i> ) for more information.

### Procedure

1. In the server's **Administration** window, click **Media**.  
Media-related topics appear in the navigation tree.
2. Select **Volumes**. The Volumes detail table appears. The following table lists the volume-related categories displayed in the Volumes detail table.

## Read-only mode

When the mode of a volume is read-only, no new data can be written to the volume. A read-only volume is not a write-protected volume. The save sets on the volume are still subject to their browse and retention policies, and the volume is not protected from being overwritten. When all the save sets on the volume have changed their status to recyclable, the mode of the volume changes to recyclable, and the volume becomes eligible for automatic recycling.

[Changing a volume's mode on page 209](#) provides information on changing the volume mode.

## Changing a volume's mode

### Procedure

1. In the server's NetWorker **Administration** window, click **Media**.
2. In the navigation tree, select **Volumes**. The **Volumes detail** table appears, showing all of the server's volumes.
3. Right-click a volume in the **Volumes detail** table, and select **Change Mode**. The **Change Mode** window appears.
4. Select a mode and click **OK**.

## Recycle volumes

A volume's retention policy can be overridden by changing it to manual recycle. One reason to change to manual recycle is when save sets must be kept on a volume longer than its retention policy specifies. A volume marked for manual recycle can be changed back to recycle automatically, so that the volume once again uses its original retention policy.

### Changing a volume's recycle policy

**NOTICE**

A volume that has been set to manual recycle retains that setting, even after relabeling. It must be explicitly reset to use auto recycle.

#### Procedure

1. In the server's **Administration** window, click **Media**.
2. In the navigation tree, select **Volumes**. The **Volumes detail** table appears.
3. Right-click a volume in the **Volumes detail** table, and select **Recycle**. The **Recycle** window appears. It names the selected volume.
4. Select the recycle policy: **Auto** (default) or **Manual**.
5. Click **OK**.

## Volume labels

The NetWorker software labels each storage volume with a unique internal label that corresponds to a pool. During backup and other operations, this label identifies the pool to which a volume belongs. NetWorker software applies a label template to create a unique internal label for each volume. The NetWorker server uses label templates and pool configuration settings to sort, store, and track data on media volumes.

**NOTICE**

Label templates are created in the **Media** task, but they are applied to volume labels in the **Devices** task. Data that exists on a tape is effectively gone after the tape has been relabeled.

Labeling a volume does the following:

- Writes a label on the volume.
- Adds the volume label to the media database.
- Prepares the tape to have data written to it.

During data recovery, the server asks for a specific volume that contains the required data, identifying the required volume by the name with which it was labeled. [Sorting Backup Data on page 283](#) provides information about label templates and pools.

## Label templates

Several preconfigured label templates are supplied with the NetWorker software. These preconfigured label templates cannot be deleted. [Naming label templates on page 301](#) provides more information about label templates and preconfigured label template.

## Labeling or relabeling library volumes

Labeling volumes in a library is time-consuming, so consider labeling volumes before it is time to back up or recover files. Library volumes are labeled in the Devices task.

### Procedure

1. In the **Administration** window, click **Devices**.
2. Open the **Libraries** folder. The **Libraries** detail table appears.
3. In the navigation pane, right-click the appropriate library and select **Label**. The selected library's details appear, including divided tables for devices and slots. The **Label Library Media** window also appears.
4. The **Default** pool name appears in the **Target Media Pool** field. To select a different pool, click the field's down arrow for a list of other pool choices. The pool determines which label template is used in labeling the volume.
5. If the volume should not be recycled automatically, click **Allow > Manual Recycle**. If **Allow > Manual Recycle** is enabled when the volume is labeled, the volume is not automatically marked as recyclable when all of its save sets have expired. Only an administrator can mark the volume recyclable.

#### **NOTICE**

A volume that has been set to manual recycle retains that setting, even after relabeling. A Manual Recycle policy cannot be changed back to Auto Recycle simply by unselecting the Manual Recycle checkbox. The volume must be explicitly reset to use auto recycle. [Recycle volumes on page 210](#) provides more information.

6. To be prompted before the existing label is overwritten, select **Prompt to overwrite label**.
7. Click **OK**. The **Library Operation** window appears, stating that the library operation has started.
8. Select **Monitoring**, then the **Operations** tab, to track the status of the label operation.
9. If **Prompt to overwrite label** was selected, right-click the label operation in the **Operations Status** window to confirm intent to overwrite the existing volume label with a new label, and select **Supply Input**.

A question window appears displaying this message:

Label <labelname> is a valid NetWorker label. Overwrite it with a new label?

10. Click **Yes** to overwrite the label with a new label, or **No** to cancel the label operation.

When a volume is relabeled, that volume is initialized and becomes available for writing again.

## Verifying the Label when volume is unloaded

If a SCSI reset is issued during a backup, the volume will rewind and NetWorker may overwrite the volume label.

To detect if the label is overwritten in this circumstance, set the Verify Label On Eject attribute in the Device resource, or the Verify Label On Unload attribute in the Jukebox resource to Yes.

When either of these attributes is set to Yes, NetWorker verifies that a volume label exists before ejecting the volume. If the volume label cannot be read, all save sets on the volume are marked as suspect and the volume is marked as full.

## Empty slots in label operations

Slots that have been intentionally left empty (such as bad slots) are skipped during labeling operations. The NetWorker software logs a message similar to: “Slot 5 empty, skipping.”

### Barcode labels

The option to label a library volume with a barcode is available during automatic device configuration. [Device configuration on page 48](#) provides more information. This option can be set in the library’s Properties tab after configuration.

Barcode labels make volume inventory fast and efficient. They eliminate the need to mount the volumes in a device. The library scans the external barcode labels with an infrared light while the volumes remain in their slots. Inventorying with barcode labels greatly reduces the time needed to locate a volume or determine the contents of a library.

Barcode labels also provide greater labeling accuracy. The labels are placed on the volumes before the volumes are loaded and scanned in the library. Once the library has scanned the barcode, the NetWorker server records and tracks the label in the media database. The NetWorker server uses barcode labels only to inventory volumes. A volume must have a label, but it need not have a barcode label.

---

#### Note

Libraries include hardware that reads barcode labels. The barcode information is then forwarded to the NetWorker server. Problems reading barcode labels indicate hardware problems. In the event of a barcode-related problem, consult the library’s documentation or the hardware vendor.

---

### Requirements for performing an inventory with barcodes

To perform an inventory by using barcodes, the following requirements must be met:

- The library must have a barcode reader.
- A barcode label must be present on the tape.
- The location field within the NetWorker media database must be correct or null. To view the location field, use the mmlocate command.

### Configuring a library to use volumes with barcodes

[Barcode labeling tips on page 213](#) provides more information.

#### Procedure

1. In the **Administration** window, click **Devices**.
2. Open the **Libraries** folder. The **Libraries** detail table appears.
3. Right-click the appropriate library, and select **Properties**. The **Properties** window appears.
4. Select the **Configuration** tab.
5. In the **Media Management** area of the **Configuration** tab, select:
  - Bar Code Reader
  - Match Bar Code Labels
6. Click **OK**.

## Using unmatched volume and barcode labels

---

### Note

If unmatched volume and barcode labels are to be used, ensure that labels are attached to the outside of the volumes.

---

### Procedure

1. Apply barcode labels to the volumes.
  2. Place the volumes with the barcode labels in the library.
  3. In the **Administration** window, click **Devices**.
  4. Open the **Libraries** folder. The **Libraries** detail table appears.
  5. Right-click the appropriate library, and select **Properties**. The **Properties** window appears.
  6. Select the **Configuration** tab.
  7. In the **Media Management** area of the **Configuration** tab:
    - Select **Bar Code Reader**.
    - Ensure that **Match Bar Code Labels** is not selected.
  8. Click **OK**. The NetWorker server uses the next available label from the label template for the volume name. It labels the volumes and records both labels in the media database.
  9. Inventory the volumes to ensure that the NetWorker server has the most current volume information.
  10. Use **Media > Volumes** to match the correct volume labels to the barcode labels. Consider making a list of the name correlations.
- 

### Note

If the barcode function is enabled, but no barcode label is affixed to the volume, an error message indicates that a barcode label does not exist.

---

## Barcode labeling tips

The NetWorker server uses volume labels and barcode labels to identify volumes. Both label types are recorded in the media database. The volume label is also recorded internally on the media (internal volume label). The NetWorker server uses barcode labels to inventory volumes, and uses volume labels to identify the volumes needed for backup and recovery. A requirement to match the volume label with the barcode label can be set in the library's Properties window.

Follow these guidelines when using barcode labels with the NetWorker software:

- When NetWorker software relabels volumes automatically, it reuses the original volume label name. A label name can be changed only if the volume is relabeled manually. The NetWorker software scans the barcode label during the labeling process and updates the media database with the new volume name and its associated barcode label.
- Do not use identical barcode labels for any of the NetWorker volumes. The use of identical labels defeats the purpose of using barcode labels, which is to facilitate the inventory process and ensure label accuracy.
- Volume names must be unique on the NetWorker server. Give each volume a unique volume label. If a second volume is labeled with an existing barcode label and the

If the Match Barcode Labels attribute in the library's properties is enabled, the NetWorker server displays an error message and does not allow the second volume to be labeled. The error message identifies the library slots containing the two volumes with identical labels and the barcode label.

To correct this problem, either apply a different label to one of the volumes and restart the labeling process, or disable the Match Barcode Labels attribute in the library's properties while labeling the second volume.

- It is not necessary to label existing volumes with barcode labels if they are stored in a vault or offsite for long periods. These volumes are rarely, if ever, inventoried.
- Before using barcode labels on existing volumes, affix the barcode labels to them. Then, load and mount each volume individually, so that the NetWorker server can match the barcode label with the existing volume label.
- Record the volume label on the tape.
- A variety of barcode labels can be purchased from third-party vendors. Choose from among numeric labels, alphanumeric labels, or a special combination of numbers and characters. Furthermore, barcode labels can be ordered to match a current volume labeling scheme.
- Use a consistent labeling scheme. If volumes are labeled with the server name and an extension such as "001," order a range of labels starting with "server\_name.001" and ending with "server\_name.100", or as wide a range as necessary. Instructions for barcode labels should be provided with the library hardware documentation. Contact the hardware manufacturer with questions about barcode labels. A consistent labeling scheme helps better organize and track volumes. It also facilitates the inventory process if all of the volumes, use barcode labels.

## Volume mounting and unmounting

A volume must be mounted before files can be backed up. If no volume is mounted at the start of a backup, an error message appears and requests that a volume be mounted.

### Mounting or unmounting a volume in a library

#### Procedure

1. In the **Administration** window, click **Devices**.
2. Open the **Libraries** folder in the navigation tree. The **Libraries** detail table appears.
3. Select a library in the navigation tree or double-click a library in the **Libraries** detail table to open the double-paned library operations view. The library's drives are listed in the **Devices** column, and its slots are listed in the **Slot** column.
4. To mount a volume:
  - a. In the **Devices** column, select the appropriate drive.
  - b. In the **Volume** column, right-click a volume to mount, and select **Mount**.
    - The Library Operation window displays this message:

```
The library operation has started.
```
    - The **Monitoring > Operations** screen displays its status.
  - c. Click **OK**.
5. To unmount the volume:
  - a. Right-click the device or the volume in the double-paned table view of the library and select **Unmount**.

- The Library Operation window displays this message:
 

The library operation has started.
  - The **Monitoring > Operations** screen displays its status.
6. Click **OK**.

## Mounting or unmounting a volume in a stand-alone tape drive

### Procedure

1. Manually insert a volume in the stand-alone drive, or ensure that a volume is already loaded.  
  
In a stand-alone device, a volume that has been loaded into the drive is not considered to be mounted until it has been explicitly mounted in the user interface or from the command-prompt.
2. In the **Administration** window, click **Devices**.
3. Select **Devices** in the navigation tree. The **Devices detail** table appears.
4. Select the appropriate device. To mount the volume, in the **Devices detail** table, right-click the device and select **Mount**.
5. To unmount the volume, in the **Devices > detail** table, right-click the device and select **Unmount**.
  - The Library Operation window displays this message:

The library operation has started.

- The **Monitoring > Operations** screen displays its status.
6. Click **OK**.

## Labeling and mounting a volume in one operation (stand-alone tape drive)

When more than one storage device is connected to the NetWorker server, the device to be used for labeling must first be selected from the list of available devices. Remember that labeling a volume makes it impossible for the NetWorker server to recover original data from that volume.

### Procedure

1. In the **Administration** window, click **Devices**.
2. Manually insert an unlabeled or recyclable volume in the NetWorker server storage device, or ensure that a volume of this type is already present for the NetWorker server to access.
3. Select **Devices** in the navigation tree. The **Devices detail** table appears.
4. Right-click the appropriate stand-alone device in the detail table, and select **Label**. The **Label** window appears:
  - a. Type a unique label name, or accept the default name associated with the selected pool.

If the volume is unlabeled, the NetWorker server assigns the next sequential label from the label template associated with the selected pool. If a recyclable volume from the same pool is being relabeled, then the volume label name and sequence number remain the same. Access to the original data on the volume is destroyed, however, and the volume becomes available.

- b. Select a pool on the **Pools** menu. The NetWorker server automatically applies the label template associated with the **Default** pool unless a different pool is selected.

- c. Select the **Manual Recycle** attribute if the volume should be manually recycled.

If the Manual Recycle attribute is enabled when the volume is labeled, the volume cannot automatically be marked as recyclable according to the retention policy. When a volume is marked manual recycle, the NetWorker server disregards the assigned browse and retention policies. Therefore, only an administrator can mark the volume recyclable.

A volume that has been set to manual recycle retains that setting, even after relabeling. A Manual Recycle policy cannot be changed back to Auto Recycle by clearing the Manual Recycle checkbox. The volume must be explicitly reset to use auto recycle. [Recycle volumes on page 210](#) provides more information.

- d. The **Mount After Labeling** attribute is selected by default. The NetWorker server automatically labels the volume, and then mounts the volume into the device.

5. Click OK.

6. If the volume is recyclable, a message warns that the named volume is about to be recycled, and asks whether to continue. Click Yes to relabel and recycle the volume.

7. After a volume is labeled and mounted in a device, the volume is available to receive data. Since the NetWorker label is internal and machine-readable, place an adhesive label on each volume that matches that internal volume label.

[Configuring a library to use volumes with barcodes on page 212](#) provides information on using barcode labels.

---

#### Note

If you are in the process of relabeling a mounted volume and you choose to not overwrite the existing label, the volume will be left in an unmounted state. To use this volume, mount it again.

---

## Labeling volumes without mounting

Volumes can be prelabeled without being mounted.

To label a volume without mounting, follow the same procedures as for labeling and mounting in one operation, but clear the Mount After Labeling attribute in the Label window.

## Mounting uninventoried volumes

You can mount volumes that are not included in the library inventory, but are valid (properly labelled) NetWorker volumes.

### Procedure

1. In the **Administration** window, click **Devices**.
2. Select **View > Diagnostic Mode** on the toolbar.
3. Manually insert the volume in an empty library slot.
4. Open the **Libraries** folder in the navigation tree. The **Libraries** detail table appears.
5. Select the library in the navigation tree in which the volume was manually inserted, or double-click the same library in the **Libraries** detail table. The **Libraries** detail table changes to the double-paned library operations view. The library's drives are listed in the **Devices** column, and its slots are listed in the **Slot** column.
6. In the **Devices** column, right-click the library in which the volume was manually inserted, and select **Inventory**. The **Inventory Library** window appears.
7. Type the slot number of the volume in both the **First** and **Last** field of the **Slot Range**.

8. Select **Operation Type**: either **Slow/Verbose** (the default) or **Fast/Silent**.

- When **Slow/Verbose** is selected, the **Supply Input** option and icon on the **Operations** screen of the **Monitoring** window can be used to confirm the choice to relabel a volume. The device path appears in the **Device** field.
- When **Fast/Silent** is selected, the **Supply Input** option and icon are not available, and relabeling proceeds automatically, without user input. The device path does not appear in the **Device** field. [Entering user input on page 439](#) provides details.

9. Click **OK**.

- The **Library Operation** window displays this message:

The library operation has started.

- The **Monitoring > Operations** screen displays its status.

The NetWorker software then inventories the specified slot.

10. Mount the inventoried volume as described in [Overview on page 33](#).

**NOTICE**

Unlabeled tapes may not be mounted for inventorying. Unlabeled tapes can only be mounted to be labeled. An attempt to mount an uninventoried volume by using unlabeled media results in an I/O error. The volume will also be ejected.

## Unmounting volumes automatically (idle device timeout)

At times, a volume that is mounted in one device might be needed by another device in the same library. For example, data being recovered by one device could span more than one volume, and the required volume could be mounted on another device. To address this need, a value can be defined in the Idle Device Timeout attribute for that particular library.

The Idle Device Timeout attribute specifies the number of minutes a mounted volume can remain idle before it is automatically unmounted from the device and returned to its slot, where it can then be accessed by another device. For libraries, this attribute appears on the Timers tab of a library's Properties. The default value for a library is 10 minutes.

### Procedure

1. In the server's **NetWorker Administration** interface, click **Devices**.
2. Open the **Libraries** folder in the navigation tree.
3. Right-click the appropriate library in the detail table, and select **Properties**. The **Properties** window appears.
4. Select the **Timers** tab.
5. Specify a value in the **Idle Device Timeout** attribute.
6. You can also override the library's Idle Device Timeout attribute for a specific device in the library.  
To specify the Idle Device Timeout value for a specific device:
  6. In the server's **Administration interface**, click **Devices**.
  7. Select **View > Diagnostic Mode**.
  8. Select **Devices** in the navigation tree. The Devices detail table appears.
  9. Right-click the device and select **Properties**.
  10. Select the **Advanced** tab.

### 11.Specify a value in the **Idle Device Timeout** attribute.

The default value is 0 (zero) minutes, which means that the device never times out and the tape must be ejected manually. However, when the value of this attribute is set to 0, the value specified in the device library's Idle Device Timeout attribute will take precedence.

## Libraries with volume import and export capability

The NetWorker software supports the use of the SCSI-II import/export feature found in many brands of library. Depending on the library model, this feature is also known as cartridge access port (CAP), mail slot, and loading port. The import/export feature deposits and withdraws (ejects) volumes from slots in the library. This feature enables the operator to deposit and withdraw cartridges without invalidating the device inventory list. Normally, if the operator opens the door to load or unload media, the element status of the autoloader is invalidated, which requires the reinitialization the library. The NetWorker server does not, however, automatically inventory the volume after a deposit and withdrawal.

The reinitialization usually consists of the following:

- An inventory of all slots
- A reset of the robotic arm
- A check to see whether each drive is working

The Deposit attribute causes a library to take the first available volume from the CAP and place it in the first empty library slot. The Eject/Withdraw attribute moves a volume from a slot (never from a drive) to the CAP.

## Depositing a volume by using the import/export feature

Use these general instructions when working with a CAP. Specific instructions for working with a CAP can vary, depending on the library manufacturer. For specific instructions, refer to the library's documentation.

### Procedure

1. Ensure that volumes are available in the CAP for deposit.
2. In the **Administration** window, click **Devices**.
3. Select **Libraries** in the navigation tree. The **Libraries detail** table appears.
4. Double-click the library in which to deposit the volume. The **Libraries detail** table changes to the double-paned library operations view.
5. Right-click either the device or the slot, and select **Deposit**. You are prompted to deposit the volume.
6. Click **Yes**. The **Library Operation** window displays this message:

The library operation has started.

The Monitoring > Operations screen displays its status.

7. Click **OK**.
8. Click **Monitoring** to go to the **Monitoring** window and select the **Operations** tab.
9. Right-click the **User Input** icon for the deposit job and select **Supply Input**. You are prompted to load the cartridges into the ports and type **Yes** to continue.
10. Click **Yes**.
11. Right-click the **User Input** icon for the deposit job and select **Supply Input** again. You are prompted to continue depositing volumes.

12. Click **Yes** to continue depositing volumes, or **No** when done.

## Withdrawing a volume by using the import/export feature

---

### Note

If the library is partitioned into logical libraries and the import/export slots are shared between the partitions, you must withdraw volumes by using the `nsrjb` command with the `-P` option to specify the port or ports from which to withdraw volumes. Refer to the `nsrjb` man page or the *EMC NetWorker Command Reference Guide* for more information.

### Procedure

1. Ensure that the volume to be withdrawn is in a known slot, and that the CAP has an empty port to hold the withdrawn volume.
2. In the **Administration** window, click **Devices**.
3. Select **Libraries** in the navigation tree. The **Libraries** detail table appears.
4. Double-click the library from which the volume is to be withdrawn. The **Libraries** detail table changes to the double-paned library operations view.
5. Right-click the slot that contains the volume, and select **Eject/Withdraw**. You are prompted to withdraw the volume.
6. Click **Yes**.
  - The Library Operation window displays this message:

The library operation has started.

  - The **Monitoring > Operations** screen displays its status.
7. Click **OK**.
8. Select **Monitoring > Log** to see the result. A successful **Eject/Withdraw** operation ends with a **Succeeded** comment in the Log.

## Inventorying library volumes

When the NetWorker software labels the contents of a library, the software registers the location of the volumes in the library slots when it assigns the volume label. This is called taking inventory. When the volumes in the library are inventoried, the NetWorker software reads the label of each volume and records its slot number. If the volumes are not moved in the library after they have been labeled, then the NetWorker server can access the volumes because each volume label is assigned to a specific slot.

If, however, the contents of the library are changed without being labeled, or if volumes are moved into new slots, the NetWorker software must be notified that the library now holds a different set of labeled volumes or that the volumes are in a different order. For example, if the library has more than one magazine, the volumes must be inventoried each time a magazine is removed and another one is loaded into the library.

When the volumes in a new magazine are labeled, there is no need to inventory them. The NetWorker software automatically records the slot number in which each newly labeled volume is located.

The NetWorker software can use barcode labels to speed up the inventory process. If the library supports the use of barcode labels, consider using them if large numbers of volumes and/or if the library contents change often. [Barcode labels on page 212](#) provides more information on using barcode labels.

### Procedure

1. In the **Administration** window, click **Devices**.
2. Open the **Libraries** folder in the navigation tree. The **Libraries** detail table appears.
3. Select a library in the navigation tree or double-click a library in the Libraries detail table. The **Libraries** detail table changes to the double-paned library operations view.
4. Right-click anywhere within the **Devices** pane, and select **Inventory**. The **Inventory > Library** window appears.
5. Type the numbers of the first and last slots to be inventoried in the **Slot Range** area.
6. Select **Operation Type**: either **Slow/Verbose** (the default) or **Fast/Silent**.
7. Click **OK**.
  - The **Library Operation** window displays this message:

The library operation has started.

  - The **Monitoring > Operations** screen displays its status.
8. Click **OK**. If the volumes do not have barcode labels, the NetWorker software must mount each volume, read its label, and unmount it. In this case, the inventory process can take some time to complete.

## Remove volumes from the media database and online indexes

The main purpose of removing volume-based entries from the online indexes is to eliminate damaged or unusable volumes from the NetWorker server. A volume entry should be removed from the media database only if the volume has become physically damaged or unusable.

Both the client file index and media database entries can be removed. This action removes all information about the volume from the NetWorker server. Even if the database entries for a volume are removed, as long as the volume is undamaged, the data remains recoverable by using the scanner program.

In general, do not remove both the client file index and media database entries at the same time unless the volume is damaged or destroyed.

The presence of a clone of the particular volume prevents the deletion of the volume entry in the media database. This is because the NetWorker server accesses the cloned volume rather than the original volume as needed. The volume's entry in the media database is never actually purged. Because of this, removing volume entries from the media database is not a particularly effective way to reduce index size, although it does reduce the size of the online indexes by purging index entries associated with specific volumes.

### Deleting volume data

The nsrmm and mminfo UNIX man pages or the *EMC NetWorker Command Reference Guide* provide more information.

### Procedure

1. In the **Administration** window, click **Devices**.
2. Open the **Libraries** folder in the navigation tree. The **Libraries** detail table appears.
3. Select a library in the navigation tree or double-click a library in the **Libraries** detail table.

- The **Libraries** detail table changes to the double-paned library operations view. The library's drives and mounted volumes are listed, as well as its slots and all volumes, mounted or unmounted.
  - Only unmounted volumes can be deleted.
4. Right-click the volume to be deleted, and select **Delete**. The **Delete** window appears and displays a request to select from where the volume should be removed:
    - a. File and media index entries
    - b. File index entries only
- NOTICE**
- 
- Do not remove the indexes of save sets on bad volumes.
- 
5. Click the appropriate selection.
  6. Click **OK**.
  7. After a bad volume has been removed, type the **nsrck** command at the command prompt.

## Marking a volume as full for offsite storage

When removing a volume from a library to store offsite, mark the volume as “full” so that the NetWorker software will not continue to ask for the volume.

To mark a volume as full, use the **nsrjb** command (for libraries) or the **nsrmm** command (for stand-alone drives) from the command-prompt. Note that the volume must be unmounted before this operation can be completed.

The format is as follows:

- For libraries:

```
nsrjb -o full volid
```

- For stand-alone drives:

```
nsrmm -o full volid
```

Where **volid** is the volume identifier of the volume. When a volume is marked as full, it is also marked as read-only.

You can also change the volume's Location attribute to an informational message. For example, Move to offsite storage in September 2009.

### Procedure

1. In the **Administration** window, click **Media**. Media-related topics appear in the navigation tree.
2. Select **Volumes**. The **Volumes** detail table, which includes information about all of the server's volumes, appears.
3. Right-click a volume in the detail table, and select **Set Location**. The **Set Location** window appears.
4. Type a location description.  
This is descriptive information. Filling in this field does not send a volume anywhere.
5. Click **OK**.

## Cloning volumes

[Volume cloning on page 329](#) provides information about volume clone operations.

# Media handling errors

The architecture of device drivers can produce media handling errors. The NetWorker software automatically retries a failed operation such as a mount or read of a volume. The number of times the NetWorker software retries the failed operation depends on the value of the Max Consecutive Errors attribute, which is set in the Advanced tab of the device's Properties window. The default value is 20. When the device's Max Consecutive Errors value is reached, the device stops retrying the operation and becomes disabled.

A mount or read operation might fail for several reasons, for example:

- Attempts to mount and read a damaged tape in a library can result in a loop of failed actions: the device might repeatedly try to mount the tape, replace it in the slot, and then retry the action with the same result. In this example, to bring the drive back into use, remove the damaged tape, then reenable the device.
- A drive that always reports a fixed number of failures before correctly mounting and reading a tape, even if the tape is not damaged, can cause a failure loop. In this example, ensure that the Max Consecutive Errors value is higher than the number of times that particular drive fails before working correctly.

## Re-enabling a device

Once the number of retries equals the Max Consecutive Errors value, the device becomes disabled. After the problem that disabled the device has been fixed, the device (drive) must be reenabled before it can be used again.

### Procedure

1. When the NetWorker computer is idle, remove any volume from the disabled drive and ensure that the drive is in good working order.
2. In the **Administration** window, click **Devices**. The **Devices** detail table appears.
3. Right-click the drive to be reenabled, and select **Properties**. The **Properties** window appears.
4. In the **Status** area of the **General** tab, set **Enabled** to **Yes**.
5. Click **OK**.
6. If the disabled drive is part of a library, it might be necessary to reset the device. To do this:
  1. From the command prompt, change the path to the directory that contains the NetWorker binaries.
  2. Type this command:

```
nsrjb -HE
```

#### NOTICE

A device retains its enabled or disabled status in the Properties window and in the Devices detail table regardless of whether its storage node is enabled or disabled. Therefore, it is possible that the storage node Properties window is set to disabled while its devices appear to be enabled in the GUI.

# Media management in a silo

More than one software application can use a single silo. Therefore, media management in a silo requires extra operations to prevent the NetWorker software from overwriting volumes used by other programs.

## Silo slot numbering

In a library, the NetWorker software specifies many functions by slot number. A library has a fixed number of slots, and NetWorker software uses the slot number to refer to a volume's physical location.

A silo works similarly, but a silo has a variable number of slots, starting at zero when it is first configured, and limited by the silo license purchased. The fundamental identifier of a silo volume is its barcode, or volser (volume serial number). The volser never changes over the life of a particular volume.

When the `nsrjb` command lists the contents of a silo, it also lists a slot number. Use the slot number to specify which volumes to mount, unmount, label, and inventory. Volumes are not always assigned the same slot number in the silo. The slot numbers in the silo are assigned dynamically, based on the sorted order of the barcodes that have been allocated. If additional barcodes that fall earlier in the sort sequence are allocated later, then the slot numbers change for all volumes that are later in the sequence.

The `nsrjb` UNIX man page or the *EMC NetWorker Command Reference Guide* provide more information.

## Silo volume mounting and unmounting

The mount and unmount operations for silos are the same as for library volumes.

Consider the following when mounting and unmounting library volumes:

- A volume must be mounted before it can be labeled, read, or had data written on it. The robotic mechanism mounts volumes in the devices of a silo.
- Volumes must be unmounted before they can be inventoried in a silo or removed from a NetWorker pool.

[Volume mounting and unmounting on page 214](#) provides more information.

## Silo volume labeling

The NetWorker labels for volumes in a silo include both a regular NetWorker volume label (written on the media of the volume) and a silo barcode identifier. The volume label is usually based on the volume pool's label template. The barcode identifier is written on a physical label on the outside of the volume, which the barcode reader in the silo can scan during inventory. [Volume labels on page 210](#) and [Barcode labels on page 212](#) provide instructions on how to label silo volumes.

The use of barcodes with matching barcode labels and NetWorker volume labels, are both available for a silo. The Barcode Reader attribute must be selected, however the Match Barcode Labels attribute is optional. When both attributes are selected, the internal volume label that NetWorker software writes on the media of each volume will match the barcode label on the outside of the volume. When the labels match, it is easier to track volumes. But the NetWorker software does not require the internal and external labels to match.

With most silo management software, unlabeled volumes can be used. The silo management software assigns a "virtual" barcode label to those volumes. Although

volumes can be used without barcodes, it is difficult to maintain integrity, since once the volume has been removed from the silo, the information about the virtual barcode is lost. Any volume without an actual barcode can be reinserted into the silo under a virtual barcode that NetWorker software (or another application) associates with some of the data.

## Using silos with volume import and export capability

NetWorker software supports the use of the import/export feature found in many brands of silos. Depending on the silo model, this feature is also known as CAP, mail slot, and loading port. The import/export feature deposits and withdraws volumes from slots in the silo.

The import/export feature enables the operator to deposit and withdraw cartridges without invalidating the device inventory list. If the operator opens the door to load or unload volumes, the element status of the autoloader is invalidated, requiring the time-consuming operation of reinitializing the silo. Note however, that NetWorker software does not automatically inventory the volume after a deposit.

Either NetWorker software or the silo management software can be used to control the import/export feature on the supported silos to deposit and withdraw volumes in a silo. But it is often more efficient to use the silo management software, especially to deposit or withdraw a large number of volumes.

On some silos (for example, StorageTek silos with the import/export feature set to automatic mode), the silo management software inserts volumes automatically. On these silos, the NetWorker software cannot be used to insert volumes.

To issue deposit and withdraw commands:

- To add and deposit volumes, type: `nsrjb -a -T tags -d`
- To remove and eject/withdraw volumes, type: `nsrjb -x -T tags -w`  
where tags specifies the tags or barcodes of volumes in a remote silo.

### NOTICE

You cannot deposit a volume from the CAP (I/O Port) using the nsrjb -d command. A silo volume deposit requires the -T and -a options in sequence to add a volume in the media database.

The sequence of operations is: nsrjb -d -T BarCode

Ignore the error message that appears. nsrjb -a -T BarCode

---

## Barcode IDs

A list of available barcode-labeled volumes is available from the silo management software. Refer to the silo manufacturer's documentation for how to generate the list of barcode IDs.

To specify a barcode identifier or template for the volumes from a command prompt, use the -T option with the nsrjb command. The nsrjb UNIX man page or the *EMC NetWorker Command Reference Guide* provides more information.

## Silo volume allocation

When volumes are added, the NetWorker server is directed to the volumes it can use.

### NOTICE

Because silos can be used by more than one software application, it is possible that a different application could read or write to volumes that belong to the NetWorker software. To prevent this from happening, most silo management software includes methods to limit access to volumes based on the hostname of the computer on which various programs run. The NetWorker software does not provide a method for setting up this sort of protection. The silo management software must configure it.

The addition of a volume causes the NetWorker software to query the silo management software to verify that the requested volume exists.

If the volume exists, the volume is allocated to the NetWorker software.

## Adding a silo volume

### Procedure

1. In the **Administration** window, click **Devices**.
2. Open the **Libraries** folder in the navigation tree. The **Libraries** detail table appears.
3. Double-click a silo in the **Libraries** detail table to open the double-paned library operations view. The silo's drives are listed in the **Device** column, and its slots are listed in the **Slot** column.
4. Right-click a silo in the **Device** column, and select **Add**. The **Add Library Volumes** window appears, with the option to select either **Template** or **List** for barcode selection.
5. Select either **Template** or **List** to enter barcode volume identifiers.
  - The **Template** option allows the use of wildcards in creating a list of barcode IDs. Each entry should be on a separate line; for example, to name four tapes A01B, A02B, A03B, and A04B, type:
 

A0  
1-4  
B
  - The **List** option allows the entry of barcode IDs, separately. Each entry should be on a separate line; for example, type the name for each tape:
 

A01B  
A02B  
A03B  
A04B
6. Type the appropriate volume identifiers in the **Barcodes** field.
7. Click **OK** (or **Cancel**, to continue adding to the list).
  - Click "+" to add an entry.
  - Click "<" to insert above a highlighted selection.
  - Click "-" to delete an entry.

The Library Operation window displays this message:

`The library operation has started.`

The Monitoring > Operations screen displays its status.

8. Click **OK**. On return to the **Library** detail table, the added volumes will be shown.

## Troubleshooting a silo

If the particular silo model does not automatically deposit the volume, then place the volumes in the insert area, right-click the volume and select Deposit.

To perform the Deposit and Add operations from a command prompt:

- On silos that require manual depositing, such as DAS:

```
nsrjb -a -T tags -d
```

where tags specifies the tags or barcodes of volumes in a remote silo. The -d flag performs the manual deposit.

- On silos where the silo management software deposits volumes automatically, such as StorageTek silos:

```
nsrjb -a -T tags
```

[NetWorker software interactions with a silo on page 146](#) provides more information on STLIs.

## Deallocating (removing) silo volumes

When an STL volume in a silo is no longer needed, the volume can be deallocated from the silo. Deallocation is basically the same operation as removing a volume from a library. Although the volume cannot be loaded by the robotic mechanism, the entries in the NetWorker media database remain intact. If the volume is allocated again, NetWorker software can retrieve the data from it later.

Use deallocation when the silo license limits the number of usable slots, or when data is moved offsite for safer storage. When the license limits the number of slots, it might be possible to leave the volumes in the silo, if it is certain that the volumes will not be used by another application. That way, the volumes can easily be added again when the data on them must be accessible.

The allocation operation is not automatic. The volumes must be manually allocated again and reinventoried to let the NetWorker server access the data. If the volume is to be removed from the silo for offsite storage, it must be removed with NetWorker software and then ejected from the silo by using the silo management software.

### Procedure

1. Unmount the volume from the device. [Volume mounting and unmounting on page 214](#) provides instructions on unmounting volumes.
  2. In the **Administration** window, click **Devices**.
  3. Open the **Libraries** folder in the navigation tree. The **Libraries** detail table appears.
  4. Double-click a silo in the **Libraries** detail table to open the double-paned library operations view. The silo's drives are listed in the **Device** column.
  5. Right-click a silo in the **Device** column, and select **Remove**.
- The Remove Library Volumes window appears, with the option to select either **Template** or **List** for barcode selection.
6. Select either **Template** or **List** to enter barcode volume identifiers.
    - The **Template** option allows the use of wildcards in creating a list of barcode IDs. For example, to name four tapes A01B, A02B, A03B, and A04B, type A0, 1-4, and B.

- The **List** option allows the entry of barcode IDs, separately. For example, type the name for each tape: A01B, A02B, A03B, and A04B.
7. Type the appropriate volume identifiers in the **Barcodes** field.
  8. Click **OK**.
    - The **Library Operation** window displays this message:

The library operation has started.

    - The **Monitoring > Operations** screen displays the silo's status.
  9. Click **OK**. Notice that on return to the **Libraries** detail table, the removed volumes are no longer listed.

### Results

[NetWorker software interactions with a silo on page 146](#) provides information on STLs.

## Inventory silos

Taking inventory of the volumes in a silo ensures that the mapping between slot number and volume name is correct, or reconciles the actual volumes in a silo with the volumes listed in the NetWorker media database.

The slot number of a silo volume is not a numbered slot inside the silo, as it is in a library. The slot number of a silo volume is the number of the volume's position in the list of volumes in a silo.

The tasks for inventorying volumes in a silo are the same as those for a library.

[Inventorying library volumes on page 219](#) provides information about inventorying a library.

The NetWorker software examines all of the volumes in the silo and compares the new list of volumes to the NetWorker media database. Then the NetWorker software produces a message listing any volumes located in the silo that are not in the media database.

When the NetWorker software inventories a silo, the silo's barcode label reader reads the barcode labels on the outside of each volume. When a barcode matches an entry in the NetWorker media database, the volume does not need to be loaded. The inventory proceeds rapidly. If, however, the NetWorker software reads a barcode that does not match any of the entries in the media database, the volume must be mounted and read in order for a proper inventory to be taken.

## Volume save sets

Information about individual save sets on volumes can be displayed from the Volumes detail table. Refer to this information to determine how resources are being used. For example, knowing the size of a save set can help in planning the amount of disk space needed for the online indexes.

## Viewing save set details in the Volume Save Sets window

### Procedure

1. In the **Administration** window, click **Media**. Media-related topics appear in the navigation tree.
2. Select **Volumes**. The **Volumes** detail table, which includes information about all of the server's volumes, appears.

3. Right-click a volume in the detail table, and select **Show Save Sets**.
4. The **Volume Save Sets** window appears. The following table shows the attributes and their descriptions.

Volume Save Sets window

Category	Description
Client	Name of the NetWorker client computer that created the save set.
Save Set	Pathname of the file system containing the save set. This column also includes clone information. If the save set has a clone, the pathname is marked has clones and the cloned save set is marked clone save set.
SSID	Save set ID number.
Time	Date and time when the save set was created.
Level	Level of backup that generated the save set. This refers only to scheduled backups. For manual backups, the level is blank.
Status	Type of save set.
Size	Save set size, in appropriate units.
Flags	<p>First flag shows which part of the save set is on the volume:</p> <ul style="list-style-type: none"> <li>• c: Completely contained on volume.</li> <li>• h: Spans volumes, and head is on this volume.</li> <li>• m: Spans volumes, and a middle section is on this volume.</li> <li>• t: Spans volumes, and the tail section is on this volume.</li> </ul> <p>Second flag shows save set status:</p> <ul style="list-style-type: none"> <li>• b: In the online index and is browsable.</li> <li>• r: Not in the online index and is recoverable.</li> <li>• E: Marked eligible for recycling and may be overwritten at any time.</li> <li>• a: Aborted before completion. Aborted save sets whose targets were AFTD or DD Boost devices are never shown in the Volume Save Sets window nor in mminfo reports because such save set entries are removed from the media database immediately.</li> <li>• i: Still in progress.</li> </ul> <p>Optional third flag:</p> <ul style="list-style-type: none"> <li>• N: NDMP save set</li> <li>• R: Raw partition backup (such as for a supported module).</li> <li>• P: Snapshot</li> </ul> <p>Optional fourth flag:</p> <ul style="list-style-type: none"> <li>• s: NDMP save set backed up by nsrdsa_save command to a NetWorker storage node.</li> </ul>

5. Click **OK** to close the **Volume Save Sets** window.

## Changing save set status within the Volume Save Sets window

You can change the save set status in the Volume Save Sets window.

### Procedure

1. Select a save set.
2. Click **Change Status**. The **Change Save Set Status** window appears.
3. Select either:
  - Normal (default)
  - Suspect
4. Click **OK**, to leave the **Change Save Set Status** window.
5. Click **OK**, again, to leave the **Volume Save Sets** window.

## Viewing save set details from the save set detail table

### Procedure

1. In the **Administration** window, click **Media**. Media-related topics appear in the navigation tree.
2. Select **Save Sets**.

The Save Sets detail table appears with two tabs for configuring save set queries and listing save set details:

- The **Query Save Set** tab
- The **Save Set List** tab

3. Select either tab. [The Query Save Set tab on page 229](#) and [The Save Set List tab on page 230](#) provide more information.

### The Query Save Set tab

The Query Save Set tab allows users to search for save sets that meet specific criteria. Click the Query Save Set tab to access these query fields:

- Query Parameters area:
  - Client Name
  - Save Set
  - Save Set ID
  - Volume
  - Pool
  - Copies
  - Save Time (a range)
- Status area:
  - All
  - Select from:
    - Browsable
    - Scanned-In
    - In-Progress

- Suspect
- Recyclable
- Recoverable
- Aborted
- Type area:
  - All
  - Select from:
    - Normal
    - Deduplication
    - NDMP
    - Snapshot
    - Raw
- Maximum level area:
  - Full
  - 1 through 9
  - All

If no save sets are found that match the query parameters, an error message appears when closing the tab:

```
No save sets were found that matched the specified query.
```

## The Save Set List tab

The Save Set List tab lists detailed save set information.

Click the Save Set List tab to view this tabular information:

- Save Set
- SSID (Save Set ID)
- Level
- Status
- Volume Name
- Type
- Client
- Size
- Files
- Pool
- Time

# CHAPTER 7

## Browse and Retention Polices

This chapter contains the following topics:

- [About browse and retention policies](#)..... 232
- [Managing the data lifecycle](#)..... 236
- [Browse and retention policies for manual backups](#)..... 240
- [Modifying the browse and retention policy on a save set](#)..... 241

## About browse and retention policies

The **browse policy** determines how long files are maintained in the client's file index on the NetWorker server. During the period of the browse policy, users can browse backed-up data from the NetWorker client computer, and select individual files or entire file systems for recovery. After the browse policy for a file is exceeded, the entry for that file is deleted.

The **retention policy** determines how long save set entries are maintained in the NetWorker server's media database. During the period of the retention policy, an entry for a save set cannot be accidentally overwritten.

For at least the period of the retention policy, you can recover a client's backed-up data by save set selection:

- No save set is considered recyclable until, at a minimum, it has exceeded its retention policy.
- No storage volume can be relabeled and overwritten until, at a minimum, all save sets on the storage volume (including save sets that depend on them) have exceeded their retention policies.

Entries for a save set can remain in the media database forever, long after the retention policy has expired. Entries are removed from the media database when these occur:

- Storage volume is relabeled.
- Entries are manually deleted.

The NetWorker server maintains one file index for each client computer (regardless of the number of Client resources configured for it), and one media database that tracks data from all clients and all save sets.

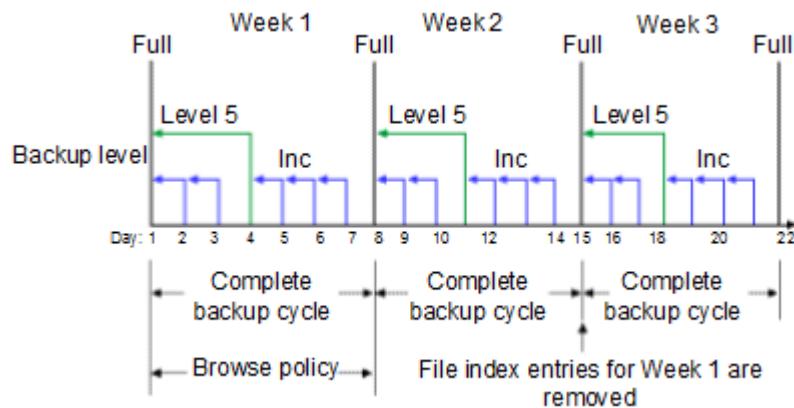
## Browse policies

You can recover a file that has an entry in the client file index by using the NetWorker client computer. Users can browse and mark files, and initiate data recovery. The NetWorker server does not remove the entry for a file until all the save sets that are dependent on the file have also exceeded their browse policies. In general, the entries for a full backup that are older than the browse policy are not removed until one backup cycle has passed. This extra time ensures that you can reconstruct a file to any point in time included in the browse policy period.

The example in this section demonstrates how a browse policy affects data availability in the client file index.

### One-week browse policy example

In the following figure, both the backup cycle and the browse policy are set at one week. A backup cycle is the length of time between full backups. Entries for the first full backup on October 1 remain in the client file index until all the dependent incremental and level 5 backups exceed the one-week browse policy. The full backup performed on October 1 is not removed until October 15, when the incremental and level 5 backups that depend on the full backup expire.

**Figure 13** One-week browse policy

To further illustrate, suppose that on October 12, you recover information that is backed up on October 5. The backup performed on October 5 is an incremental backup that is dependent on the October 4 backup, which is a level 5 backup. The October 4 (level 5) backup, in turn, is dependent on the full backup performed on October 1.

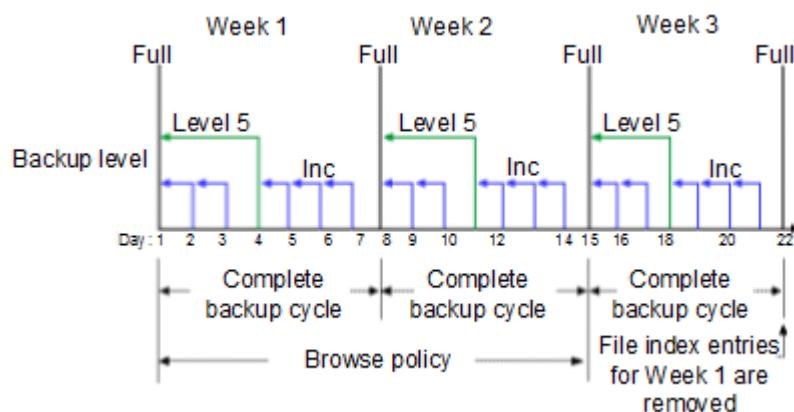
The entry for the full backup performed on October 1 must remain in the client file index for a period of time equal to the sum of the following:

- The browse policy (one week)
- One complete backup cycle (one additional week)

That is, it must remain in the client file index until the level 5 backup on October 4 and all incremental backups dependent on the full backup pass their browse policy. The entries from the Week 1 backup cycle are removed from the client file index on October 15.

### Two-week browse policy example

In the following figure, the browse policy is two weeks, which is twice as long as the backup cycle (one week). In this example, on October 18 a user can still find browsable entries in the client file index from backups created on October 4. The backup performed on October 5 is an incremental backup dependent on the October 4 backup, which is a level 5 backup. The October 4 (level 5) backup, in turn, is dependent on the full backup performed on October 1.

**Figure 14** Two-week browse policy

**Figure 14** Two-week browse policy (continued)

The full backup performed on October 1, and the incremental and level backups that depend on it, must remain in the client file index for a period of time equal to the combination of the following:

- The browse policy (two weeks)
- One complete backup cycle (one additional week)

In this example, entries for the Week 1 backup cycle are not removed from the client index until October 22.

## Retention policies

The NetWorker media retention policy specifies a period during which backed-up data is protected from an accidental overwrite. After the retention period is exceeded, the save set is eligible to change its status from recoverable to recyclable. The term recyclable means “eligible for recycling.” The save set’s status, however, does not change to recyclable until it, and all the save sets that depend on it, have passed their retention policy. The NetWorker server keeps track of save set dependencies regardless of whether the dependent save sets are stored on the same or different volumes. The expiration of a save set’s retention policy does not remove the save set’s entries from the media database.

A storage volume becomes recyclable when:

- The retention policy for every save set on a volume expires.
- The status for every save set on a volume changes from recoverable to recyclable.

Since a volume can contain save sets from multiple backup sessions, all with different retention policies, the mode of a volume might not change to recyclable for a long time. All the data on the volume remains available for recovery by using either save set recover or the scanner program. All the entries for recyclable save sets remain in the media database.

If a volume contains one or more deduplication save sets, the resource for the deduplication node that was used to create the backup must exist when the save sets pass their retention time. If the resource for the deduplication node has been deleted, the volume cannot be made recyclable or relabeled. Furthermore, when deduplication save sets pass their retention time, the NetWorker server will begin the process of deleting the deduplicated data from the deduplication node. Therefore, deduplication data may not be recoverable using the scanner program once the deduplication save set has passed its retention time.

The change in status to recyclable means that the volume can be overwritten if conditions are right. The volume can be relabeled under the following conditions:

- The volume is placed in an autochanger or mounted in a stand-alone device.
- The Auto Media Management attribute in the Device resource is enabled.

The existing data is nonrecoverable after the volume is relabeled.

Save set entries are also removed from the media database when they are manually deleted. However, the data on that volume is still available for recovery by using the scanner program. The scanner program retrieves the information needed to re-create entries in either the client file index, in the media database, or in both places:

- If you re-create the entries in the client file index, a user with the proper permissions can recover data by using the NetWorker client computer.

- If you re-create the save set's entries in the media database, a UNIX root user or a member of the Windows Administrators group can recover data by using save set recovery.

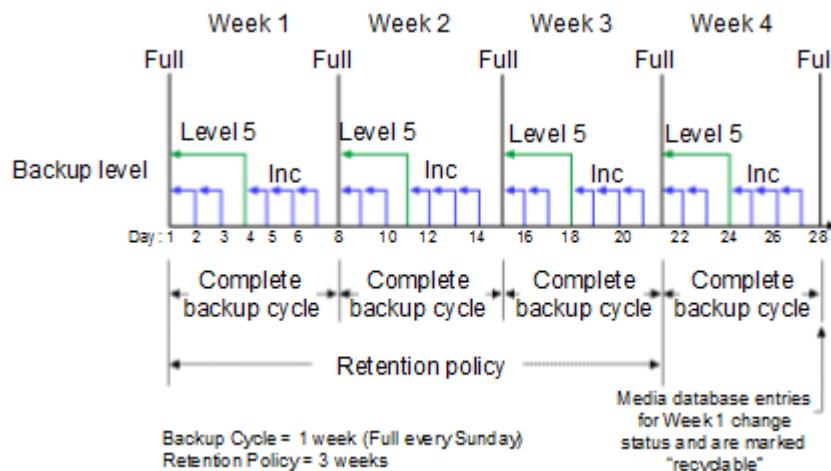
**Note**

If only one full browsable saveset backup exists, then its browse policy is equal to its retention policy.

### Three-week retention policy example

The following figure illustrates how a retention policy works. In this example, the backup cycle is set at one week and the retention policy is set at three weeks.

**Figure 15** One-week backup cycle and three-week retention policy



The save set entries for Week 1 have passed their browse policy and retention policy, but they remain available for recovery by using the scanner program or via a save set recovery until you relabel the volume. When all the save set entries on a volume change status to recyclable, the volume mode changes from full or appendable to recyclable, and the volume is ready to be relabeled for reuse.

**NOTICE**

Once a volume is relabeled, data on the volume cannot be recovered.

### Retention policies for client file index save sets

The client file indexes that reside on the NetWorker server are backed up as are any other files. However, the retention policy for these files is calculated differently than for other files. The retention policy for a client file index is based on the retention policy that is specified for the NetWorker client to which the client file index corresponds. For example, if NetWorker client jupiter has a retention policy of seven years, then the client file index that corresponds to jupiter will also have a retention policy of seven years regardless of any retention policy that may be set up for the NetWorker server. This ensures that if a NetWorker client is recovered, the corresponding client file index can also be recovered.

## Retention policies and media pools

A retention policy can also be specified for a media pool. If the retention policy is specified for a media pool as well as the client, the NetWorker software will be the longer of the two policies.

Assigning a retention policy to a clone pool has special implications. When a retention policy is specified in a clone pool, all save sets that are directed to the clone pool take on the retention policy of the clone pool regardless of the retention policy of the save set client.

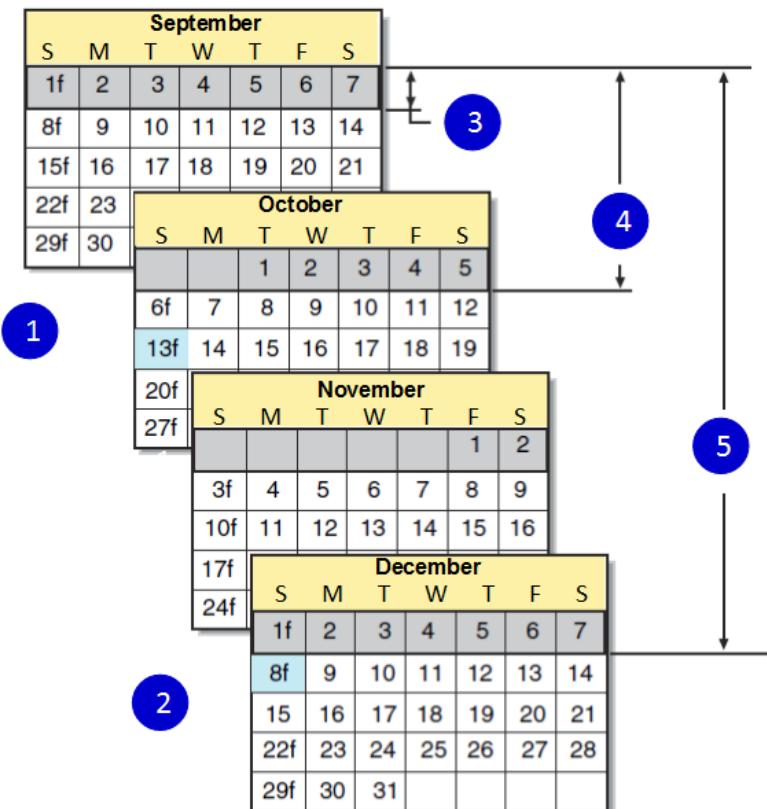
When browse and retention policies are specified with a command line program, such as `save -w -y`, the browse and retention policies are taken from that program.

## Managing the data lifecycle

Browse and retention policies control the growth of the client file index and the media database, and how long data remains available for recovery.

This figure traces the data lifecycle through the client file index and the media database. .

**Figure 16** Data lifecycle in the client index and the media database



The numbers in this figure represent the following:

1. File index entries from September 1-9 are removed.
2. Save set entries in the media database from September 1-9 change status to recyclable.
3. Backup cycle is 1 week.

**Figure 16** Data lifecycle in the client index and the media database (continued)

4. Browse policy is 1 month
5. Retention policy is 1 quarter.

In the example, the entries for the September 1 through September 7 backup cycle remain in the client index for one month (the browse policy), plus the length of a full backup cycle (one week), to ensure that all dependent entries pass their browse policies. In this case, the file index entries for the September 1 through September 7 backup cycle are removed on October 13. Since the entries exist in the client file index, you can browse and recover the data through the NetWorker client computer. As long as the save set's file entries remain in the client file index, the status of the source save set is browsable. After the save set status changes from browsable to recoverable, you must know the full path to the file in order to recover it directly.

The status for each save set backed up during the September 1 through September 7 cycle remains recoverable until their retention policies expire and all the dependent save sets exceed their retention policies. In this case, the entries from the September 1 through September 7 backup cycle change from recoverable to recyclable on December 8. When all of the save set entries on a volume change status to recyclable, the mode of the volume changes to recyclable and the volume can be overwritten.

While a save set is either recoverable or recyclable, you can recover any save set by using either the save set recovery procedure or the scanner program. Alternatively, you can use the scanner program to re-create a save set's entries in the client file index, which enables file recovery directly from the NetWorker client computer.

On October 13, all data entries from September 1 to September 7 are removed from the client file index. On December 8, the save set entries from September 1 to September 7 in the media database change status from recoverable to recyclable. After all save sets on a volume change status from recoverable to recyclable, the volume mode changes to recyclable. After the volume is relabeled, all existing data on the volume is unavailable for recovery.

#### **NOTICE**

When you relabel a volume for reuse within the same pool, the volume identification (the volume name as it appears on the volume label) remains unchanged. Even though the volume has the same label, information required by the NetWorker server to locate and restore data on the volume is destroyed. All existing data is inaccessible and will be overwritten.

## Assigning multiple policies to a single client

Identical versions of a client and save set combination can have a different set of browse and retention policies assigned for each different backup group to which it belongs. If you create an identical Client resource with the same name and save set values, but assign it to a different backup group, you can designate a different set of browse and retention policies. The NetWorker server employs the Browse Policy and Retention Policy attributes that correspond to the unique combination of the Client resource's Name, Save Set, and Group attributes.

### Assigning different policies for an identical client example

You have a Client resource for the host saturn. The Client resource has a save set value of All and is assigned to backup group general. The browse policy is weekly and the

retention policy is monthly. You create a copy of the Client resource for saturn, but assign it to the backup group special. This version of saturn has a browse policy of Weekly and a retention policy of yearly.

- If the group special is backed up, then the weekly and yearly policies are applied.
- If the group general is backed up, then the policies weekly and monthly are used.

## Preconfigured time policies

NetWorker software contains these preconfigured browse policies:

- Day
- Week
- Month
- Quarter
- Year
- Decade

You can use these preconfigured policies, or customize policies to best suit data storage needs. Create the customized policy before you configure the client. Otherwise, the policy name does not appear in the Client dialog box as an option.

## Editing a time policy

You can edit a time policy, but you cannot change the name of a time policy. To rename a time policy, delete the current time policy and create a new one.

### Procedure

1. In the **Administration** window, click **Configuration**.
2. In the expanded left pane, select **Time > Policies**.
3. In the right pane, select the time policy to edit.
4. From the **File** menu, select **Properties**.
5. Make any necessary changes in the **Properties** dialog box and click **OK**.

## Deleting a time policy

---

### Note

Preconfigured time policies cannot be deleted.

### Procedure

1. In the **Administration** window, click **Configuration**.
2. In the expanded left pane, select **Time Policies**.
3. In the right pane, select the time policy to delete.
4. From the **File** menu, select **Delete**.
5. When prompted, click **Yes** to confirm the deletion.

## Snapshot policies

A snapshot policy is required to perform backups with the NetWorker Snapshot Management (NSM) feature. This policy determines how many snapshots are created,

retained, and backed up to permanent storage. You can specify a preconfigured policy or create a custom snapshot policy.

The snapshot policy works in conjunction with the Interval attribute of the Group resource. The value for the Interval attribute must be set low enough that the specified number of snapshots can be created in the 24-hour period. For example, to create four snapshots, the Interval value must be set to six hours or less.

For more information on the NSM feature and creating a snapshot policy, refer to the *EMC NetWorker Snapshot Management Integration Guide*. The *EMC NetWorker Module for Microsoft Applications Administration Guide* provides information about creating a snapshot policy for the VSS Client.

## Working with snapshot policies

This section provides information about preconfigured snapshot policies, as well as instructions for creating, editing, and deleting snapshot policies.

### Preconfigured snapshot policies

If a new customized snapshot policy is *not* manually created, the NetWorker software provides two preconfigured policies that can be used with the snapshot management feature:

- **Rollover-only**  
With the Rollover-only snapshot policy, a single snapshot is taken per day. The data is then backed up to conventional storage media and the snapshot is deleted.
- **Daily**  
With the Daily snapshot policy, eight snapshots are taken in a single day. The data in the first snapshot is backed up to tape. Each snapshot has an expiration policy of 24 hours.

---

#### Note

Neither preconfigured snapshot policy may be deleted.

---

### Creating a snapshot policy

#### Procedure

1. In the **Administration** window, click **Configuration**.
  2. In the expanded left pane, select **Snapshot Policies**.
  3. From the **File** menu, select **New**.
  4. In the **Create Snapshot Policy** dialog box, type a name for the snapshot policy in the **Name** attribute and complete other attributes as appropriate.
- 

#### Note

For information about how to complete the attributes for a snapshot policy, refer to the *EMC NetWorker Snapshot Management Integration Guide*.

---

5. Click **OK**.

### Editing a snapshot policy

#### Procedure

1. In the **Administration** window, click **Configuration**.

2. In the expanded left pane, select **Snapshot Policies**.
3. In the right pane, select the snapshot policy to edit.
4. From the **File** menu, select **Properties**.
5. Make any necessary changes in the **Properties** dialog box and click **OK**.

## Copying a snapshot policy

### Procedure

1. In the **Administration** window, click **Configuration**.
2. In the left pane, select **Snapshot Policies**.
3. In the right pane, select the **Snapshot Policy** resource to copy.
4. From the **Edit** menu, select **Copy**. The **Create Snapshot Policy** dialog box appears.
5. Type the name for the new **Snapshot Policy** resource in the **Name** attribute, edit any other attributes as appropriate, and click **OK**.

## Delete a snapshot policy

### Procedure

1. In the **Administration** window, click **Configuration**.
2. In the expanded left pane, select **Snapshot Policies**.
3. In the right pane, select the snapshot policy to delete.
4. From the **File** menu, select **Delete**.
5. When prompted, click **Yes** to confirm the deletion.

## Browse and retention policies for manual backups

If a browse or retention policy is specified with a manual backup from the command prompt, the browse or retention policy takes effect for all of the save sets included in the manual backup. Specify browse and retention policies with a manual backup from the command prompt by using the save -w -y command. Both the browse and the retention policies must be entered in time and date formats accepted by the nsr\_getdate program. The *EMC NetWorker Command Reference Guide* or the UNIX man pages provide more information about save and nsr\_getdate.

If a browse or retention policy is not specified for a manual backup, the policies are determined as follows:

- **Browse policy**  
The save sets included in a manual backup adopt the browse policy of the Client resource. If there are multiple Client resources for the NetWorker host, the Client resource with the longest browse time is adopted. For example, if there are three Client resources for the NetWorker client mars, each with one of these browse periods:
  - One week
  - One month
  - One year
 A manual backup of mars adopts a browse policy of one year.
- **Retention Policy**  
The save sets included in a manual backup adopt the retention policy of the Client resource according to the same rules that were described previously for browse

policies. However, if a retention policy is set up for the media pool to which the backup is directed, the retention policy will be the longer of either:

- The Client resource retention policy
- The media pool retention policy

#### Note

There are special considerations for retention policies and clone data.

## Modifying the browse and retention policy on a save set

Use the nsrmm program to modify the browse and retention policy of a save set after the backup has occurred. Use nsrmm with these options.

- -e retention\_time – updates retention time
- -w browse\_time – updates browse time

Use the -e and -w options with the nsrmm option -S (to specify a save set ID).

#### Note

The retention time must be later than the browse time, and the browse time must be later than the insertion time. The insertion time is the time that the save set record was most recently introduced into the save set database.

When the -e and -w options are used with nsrmm, these must be true:

- Retention-time is greater than the browse-time.
- Browse-time is greater than the insertion-time.

Both the browse and the retention policies must be entered in time and date formats accepted by the nsr\_getdate program. The *EMC NetWorker Command Reference Guide* or the UNIX man pages provide more information about nsrmm and nsr\_getdate.

## Changing browse and retention policies with nsrmm examples

The examples in this section use nsrmm to change browse and retention policies.

- To change the retention time to midnight, January 1, 2016 and to change the browse time to midnight, January 1, 2012, type the following command:

```
nsrmm -S 3315861249 -e "01/01/09 23:59:59" -w "01/01/08 23:59:59"
```

- To change the browse time to six months from the current date and time, type the following commands:

```
nsrmm -S 5315861249 -w "6 months"
```

- To change the retention time to two years from the current date and time, type the following commands:

```
nsrmm -S 3315861249 -e "2 years"
```

## Reports on browse and retention policies for save sets

The mminfo command can be used with the -p option to display a report on the browse and retention times for save sets. The *EMC NetWorker Command Reference Guide* or the UNIX man pages provide more information about mminfo.



# CHAPTER 8

## Backup Groups and Schedules

This chapter contains the following topics:

- [Overview of NetWorker scheduling](#)..... 244
- [Backup groups](#)..... 244
- [How to manage backup groups](#)..... 253
- [Open file backups](#)..... 255
- [Schedules](#)..... 256
- [Backup levels](#)..... 263

## Overview of NetWorker scheduling

Together, the following two items enable the scheduled backup of client data:

- Group
- Schedule

Time-based groups (backup groups) specify either the time of day when a backup occurs, or a probe-based backup that is user defined.

For time scheduled backups, times typically occur after regular work hours. All clients assigned to a group will be backed up at the time specified by the backup group. Schedules enable you to specify the day of the week or month that the backup occurs, as well as the level of backup (full, incremental, synthetic full or level 1-9).

For probe-based backups, the probe interval and backup window are used to schedule group probes with clients, and clients with groups. The execution of the probes determines if the backup of the group will proceed.

---

### Note

Each client in a group can have a probe associated with it, but a probe is not required. However, a probe-based backup group must have at least one probe-enabled client associated with it.

---

## Backup groups

Time-based backup groups specify the starting time for a client's scheduled backup. These backup groups enable you to:

- Schedule the backups to take place in the middle of the night, or some other time when network traffic is low.
- Balance the backup loads by grouping clients in specific groups and staggering their start times.

### NOTICE

---

Do not place both regular and deduplication clients in the same group.

---

- Sort data to specific backup volumes.  
To sort data, groups are used in conjunction with backup pools.

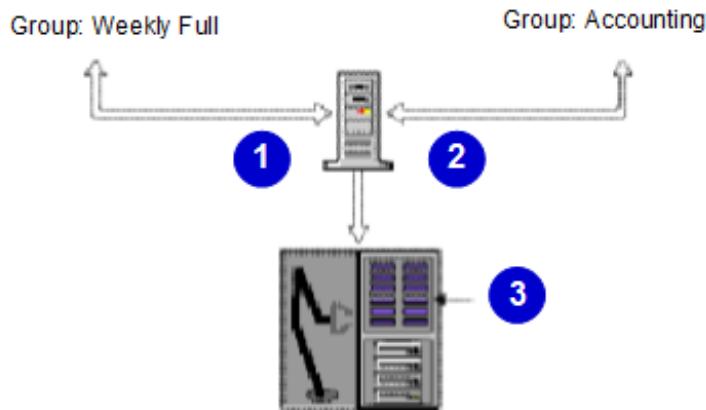
## The NetWorker server and time-based backup groups

When a Client resource is created, it is assigned to a backup group. The clients in each time-based backup group begin their automatic scheduled backups according to the start time of the group. Backup loads are balanced by taking the client's backup schedule into account when determining which clients to include in a specific group.

Use groups to balance client backups should we change the example to synthetic full

The following figure illustrates how the NetWorker server uses two time-based backup groups to back up multiple client save sets.

**Figure 17** How NetWorker groups are used to back up multiple clients



In this figure, the numbers represent the following:

1. The NetWorker servver writes data to an appropriate storage volume
2. NetWorker scheduled backup
3. Labeled media volumes

The three client computers (mars, jupiter, and saturn) in this figure are part of a group named Weekly Full. The Weekly Full group starts its automatic scheduled backup at midnight.

- Client mars runs a full backup of all its save sets every Monday and incremental backups of its save sets on the other days.
- Client jupiter runs a full backup of all its save sets on Tuesday and incremental backups on the other days.
- Client saturn runs a full backup of all its save sets on Wednesday and incremental backups on the other days of the week.

Because each client runs its full backup on a different day of the week, the server is not overloaded.

The second group, Accounting, illustrates how you can group clients by department. The Accounting group contains client computers mercury and venus, and starts its backups at 7:00 P.M., when the computers in that department are available for backup. Although the two client computers run full backups on the same day, computer venus is scheduled to perform a full backup on only the /usr/home save set, whereas all the save sets on computer mercury are backed up. By estimating how long a backup takes, you can determine the start time to set for the next group.

The save sets from each group are written to appropriate volumes mounted on storage devices. The NetWorker server uses pools to organize, track, and store save sets. The server uses groups to determine the time clients start their scheduled backups.

## Preconfigured groups

The NetWorker product ships with a single preconfigured group named Default. To ensure that all data is backed up, the NetWorker server automatically adds all clients to the Default group. However, you must enable the Default group for the NetWorker server to back it up. You can keep a client in the Default group, or you can put the client in one or more customized groups.

You can also make changes to any Default group attribute, but you cannot delete the group. You can, however, create or delete as many customized groups as required.

## Key Group attributes

The following table displays some of the key attributes for the Group resource.

**Table 31** Group attributes

Attribute	Description
Start Time	The Default group is preconfigured to start its daily backup at 3:33 A.M. This time can be changed.
Autostart	Specifies whether the group starts automatically at a designated start time. You must enable the Autostart attribute for the Default group, and any other group you create, before a scheduled backup can be run.
Schedule	This optional attribute can be used to select a Schedule resource for the group. If this attribute is set, it overrides the schedules selected in the Client resource's Schedule attribute for all clients in this group.
Interval	This attribute dictates how often a group starts a scheduled backup. The default value is 24:00 (once a day), but you can change this value to start backups more often.
Autorestart	Specifies whether the group will automatically restart after an incomplete backup due to a power failure or administrator intervention. If this attribute is enabled, the backup will restart when the NetWorker server restarts provided that the period of time specified in the Restart Window attribute has not elapsed.
Restart Window	For either auto or manual restarts, this attribute specifies the period of time in which an incomplete backup can be restarted. If the period of time has elapsed, the restart will be treated as a regular backup start operation. The restart period is calculated from the beginning of the start of the last incomplete backup. The default value is 12:00 hours.
Client Retries	When the NetWorker server fails to connect to a client, this attribute specifies the number of times that the server will reattempt the connection before the backup is considered a failure. The first retry will not occur until after an attempt has been made to at least contact each client in the group.
Inactivity Timeout	This attribute specifies the maximum time, in minutes, that a client is given to fail to communicate back to the server. If a client fails to respond beyond the Inactivity Timeout value, the server will consider the client as having failed. If a client fails due to any reason, a retry is initiated immediately. This ensures that no time is lost during the scheduled backup due to any failures.

**Table 31** Group attributes (continued)

Attribute	Description
	For large save sets, for save sets with large sparse files, and for incremental backups of a large number of small static files, increase the timeout value if the backup consistently aborts due to an inactive job.
Soft runtime limit	This attribute indicates the time, in minutes, since the start time of a given group after which no new child process will be launched. The Soft runtime limit is measured for each savegroup separately. Index and bootstrap saves are exempt and will start regardless of this setting. The default value is 0, which indicates that no Soft runtime limit is in effect.
Hard runtime limit	This attribute indicates the time, in minutes, that any save session still running is ended and the savegrp program stopped. The default value is 0, which indicates that no Hard runtime limit is in effect.
Success Threshold	This attribute sets the criteria for reporting the success of all save sets within a group. The default value is Warning, which means if any save set completes with warnings it will be reported as successful. The client will also be reported as successful with warnings in the completion report. If set to "Success", any save sets completed with warnings will be reported as failures. The client will also be reported as failed in the savegroup completion report. Any failures will attempt a retry of the save set if the retry count is not 0.
Probe based backup	If this attribute is set to ON, the probe attributes listed below become enabled. Boolean ON/OFF. It is OFF by default.
Probe interval	This attribute indicates how often probes in minutes, should be run. Default value is 60 minutes.
Probe start time/probe end time	Probe start time and probe end time together define the backup window. Probe end time minus probe start time should be greater than the probe interval. Start time default: 0:00; end time default: 23:59
Probe success criteria	This attribute determines if all probes or only one probe needs to succeed for a backup to proceed. Values are Any or All.
Time since successful backup	If the value is 0, the time since the last successful backup does not matter: the savegrp program always runs probes. If the interval is specified and reached, savegrp runs the backup regardless of the result of all other probes. The probes are run so that the probe state data can be updated. The default value is 0 days.
Time of the Last Successful Backup	Set to the time of the last successful backup by the savegrp program. Used to calculate interval since the last successful backup. GUI read only.
savegrp Parallelism	Maximum number of save sets that can be backed up simultaneously by a NetWorker group. The default value is 0, which means that parallelism is not restricted.

## Probe Group

Probe-based backup groups specify probe interval, and backup window to schedule the group.

Probing occurs continuously throughout the probing window (the hours defined Probe start time, and Probe end time), and only when the Autostart attribute of the save group

is enabled. If a save group is started manually, probes run immediately. If autostart is used, then probes only run during the specified probe window.

Clients are associated with probe-based backup groups in the same manner as they are with regular backup groups. However, probe-based backup groups must include at least one client, which references a probe resource.

Each client can reference only one probe, but since backup groups can contain many clients, multiple probes can be run with the group.

Instead of a start time, the probe start and end times are used to schedule the group. It is the outcome of the probing which determines if the backup will proceed.

#### Note

Each client in a group can have a probe associated with it, but a probe is not required. However, a probe-based backup group must have at least one probe-enabled client associated with it.

## Configuring a probe-enabled group

Configure a probe-enabled group in the server Administration interface.

#### Procedure

1. In the server **Administration interface**, click **Configuration**.
2. Right-click **Groups**, and select **New**.
3. In the **Advanced** tab of the **Create Groups** window, complete the fields in the **Probe** section as described in the following table.

**Table 32** Probe group fields

Field	Description
Probe-based group:	Click the checkbox to enable probing.
Probe interval:	Determines the frequency of probing. Can be set from a minimum of 15 to a maximum of 10,000 minutes. A successful backup does not disable probing. Be sure to set the Probe interval to an appropriate value.
Probe start time:	The time at which probing will begin.
Probe end time	The time at which probing will end.
Probe success criteria	<ul style="list-style-type: none"> <li>• Any: Any one of the probes associated with the group must succeed for the backup to be performed.</li> <li>• All: All of the probes associated with the group must succeed for the backup to be performed.</li> </ul>
Time since successful backup	The longest period of time tolerated without a backup.

## Aborted backup groups

If the backup of a save set fails, then the NetWorker server marks the save set as ABORTED. In this situation, the automated report from the savegrp program does not always show that the backup has completed. For example, if the client is being backed up over a Network File System (NFS) connection and the NFS server crashes and reboots,

the NetWorker backup hangs until it times out. The NetWorker server marks the save set ABORTED.

#### Note

Aborted save sets whose targets are AFTD or DD Boost devices are never shown in the Volume Save Sets window nor in mminfo reports because such save set entries are removed from the media database immediately.

## Creating a group for backup clients

A backup group specifies the time of day when a backup occurs.

Creating groups for backup clients enables you to:

- Balance backup loads to reduce the impact on your network and the NetWorker server.
- Sort data to specific backup volumes. To sort data, groups are used in conjunction with backup *pools*.

#### Procedure

1. From the **Administration** window, click **Configuration**.
2. In the expanded left pane, select **Groups**.
3. From the **File** menu, select **New**.
4. In the **Name** attribute, type a name for the group.
5. In the **Comment** attribute, type a description of the group.
6. For the **Start Time** attribute, type a new time, unless it is appropriate to maintain the default time of 3:33 A.M. Ensure that start times for different groups are far enough apart so that one group has completed backing up before the next group starts.
7. For the **Autostart** attribute, select **Enabled**.
8. In the **Printer** attribute, type the name of the printer on which bootstrap save set information will be printed.

## Editing a group

Edit a group from the Administration window.

#### NOTICE

You cannot change the name of an existing backup group.

#### Procedure

1. From the **Administration** window, click **Configuration**.
2. In the expanded left pane, select **Groups**.
3. Select the group to be edited.
4. From the **File** menu, select **Properties**.
5. Edit the attributes of the group and click **OK**.

## Deleting a group

Delete a group from the Administration window.

**NOTICE**

You cannot delete the preconfigured Default group nor any group currently applied to a Client resource.

---

**Procedure**

1. From the **Administration** window, click **Configuration**.
2. In the expanded left pane, select **Groups**.
3. Select the group to be deleted.
4. From the **File** menu, select **Delete**.

## Copying a group

Copy a group from the Administration window.

**Procedure**

1. From the **Administration** window, click **Configuration**.
2. In the expanded left pane, select **Groups**.
3. In the right pane, right-click the group to be copied and select **Copy**. The **Create Group** dialog box appears, containing the same information as the group that was copied, except for the Name attribute.
4. In the **Name** attribute, type a name for the new group.
5. Edit the attributes and click **OK**.

## Copy a group with clients

The Copy with Client feature allows you to copy an existing group resource including the associated group and all client resources. The Copy with Clients operation enables the following actions:

- Copy an existing NSR group.
  - Ensure the original client list is preserved in the new group.
  - All NSR client resources are automatically updated.
- 

**Note**

The Copy with Clients operation is only available to a NSR group resource type. Consequently, this functionality is only available if a NetWorker group is selected in the configuration window in the NetWorker Console.

---

The Copy with Clients option is available in the Edit menu. The option is also available in a pop-up menu that appears when an individual group is selected in the details pane or navigation tree.

## Setting the backup group time interval

The NetWorker server allows you to run an individual scheduled backup group more than once within a 24-hour period. The Interval attribute value of the Group resource determines the frequency (in hours) that an individual group will start a backup.

The default value is 24 hours (24:00), which results in one backup group run per day. If you set the Interval attribute value at 12 hours, then the same group will back up twice a day. For example, a group with the default start time of 3:33 A.M. and an interval of 12:00 would back up twice a day, first at 3:33 A.M., and then again twelve hours later at 3:33 P.M.

---

### Note

An increase in the backup group time interval (for example, changing the interval from once every 24 hours to once every 12 hours) can add strain on a network, the NetWorker server, and associated devices.

---

### Procedure

1. From the **Administration** window, click **Configuration**.
2. In the expanded left pane, select **Groups**.
3. Select the group to edit.
4. Select the **Advanced** tab.
5. In the **Interval** attribute, type a value in the hh:mm format.

For best results, use time interval values that make it easy to determine the backup group time, such as 24, 12, or 6 hours.

6. Click **OK**.

## Limiting full backups when the time interval is less than 24 hours

For groups that have more than one scheduled backup within a 24-hour period, use the Force Incremental attribute to prevent more than one full or level backup per 24-hour period.

By default, the Force Incremental attribute is set to Yes. If the Force Incremental attribute is set to Yes, the first backup is performed at the configured level. All subsequent scheduled backups during the next 24 hours after the start of the first backup are incremental. This means that only changed files are backed up regardless of the configured level. The Force Incremental attribute applies only to scheduled backups that the NetWorker server runs automatically. If the savegrp program is run by other means, such as from the command prompt or a script, this attribute is not used.

If the Force Incremental attribute is set to NO, multiple full or level backups are allowed during the 24 hours after the start time of the first backup.

## Forcing an incremental backup

Use the Force Incremental attribute to force incremental backups on groups.

### Procedure

1. From the **Administration** window, click **Configuration**.
2. In the expanded left pane, select **Groups**.
3. Select the group to edit.

4. Select the **Advanced** tab.
5. Select the **Force Incremental** attribute and click **OK**.

## Considerations for running a backup group from the command line or a script

Instead of scheduling a backup group through the NetWorker Administration window or through the nsradmin program, you can use the savegrp program to back up a group directly from the command line or from a script.

However, there are some considerations that you need to be aware of when you run the savegrp program in this way. When the savegrp program is executed directly from the command line or from a script, some attributes that may have been specified for the backup group resource through the NetWorker Administration Group Properties window or the nsradmin program will not take effect. You must specify these options directly on the command line or in the script if you want to include these options with your group backup.

For example, suppose that a backup group resource named Accounting is set up in the NetWorker Administration window. The Accounting backup group is specified to use a schedule named *Full Every Friday*. If you back up the Accounting group from a command line or a script, then you must specify the schedule explicitly by using the -C option, for example:

```
savegrp -C "Full Every Week" Accounting
```

The following table lists the backup group resource attributes and the corresponding savegrp option that must be specified explicitly on the command line or in a script if they are required for your backup group. For more information on these options, refer to the *EMC NetWorker Command Reference Guide* or the UNIX man pages.

**Table 33** savegrp options that are not taken from backup group resource attributes

For this attribute from the Group Properties window or nsradmin program...	Use this savegrp program option	Description
Level	-l	Backup level
Force incremental	-l incr	Forces an incremental level backup. The Force incremental attribute behaves differently than the -l incr option. The Force incremental attribute only forces an incremental if the group is scheduled to backup more than once in a 24 hour period. The -l incr option forces an incremental backup every time.
Printer	-P	Printer to which bootstrap information will be printed
Schedule	-C	Backup schedule
Schedule time	-t	Specifies an explicit time when looking at a schedule to determine what level of save to perform. No value means use the current date to determine the level.
Savegrp parallelism	-N	Parallelism for the backup group. The parallelism attribute is taken from the backup group resource if no value is specified with -N or if the

**Table 33** savegrp options that are not taken from backup group resource attributes (continued)

For this attribute from the Group Properties window or nsradmin program...	Use this savegrp program option	Description
		value specified with -N is 0 (unlimited parallelism for the backup group).
Expiration time	-w -y	-w specifies browse time -y specifies retention time
Verbose	-v	savegrp job information detail level
Estimate	-E	Estimate amount of save data before performing a save
No save	-n	Estimate amount of save data but do not perform a save
No monitor	-m	Do not report on status of savegrp operation
Index only	-O	Save only each client index and bootstrap
Preview	-p	Run a probe step on each client but do not save data
Revert to full when synthetic full fails	-F	Automatically perform a full level backup if a synthetic full backup operation fails.
Verify synthetic full	-V	If a synthetic level backup is performed, verify that synthetic full save sets are indexed (available for browsing) after the save sets are created.

## How to manage backup groups

The following topics provide information about how to manage backup groups.

### Previewing a backup group

Preview a backup to identify potential problems before the NetWorker server runs a backup group.

You can simulate a backup for a specific group. This feature generates an output that includes this information:

- File System to be backed up
- Backup level
- Backup pool

#### Procedure

1. From the **Administration** window, click **Configuration**.
2. In the expanded left pane, select **Groups**.
3. Select the group to edit.
4. Select the **Advanced** tab.

5. In the **Option** attribute, select **Preview** and click **OK**.

#### Results

To see the simulated results of the backup, open the daemon log file located in the <NetWorker\_install\_dir>\logs directory.

## Moving clients between groups

You can move multiple clients from one group to another.

#### NOTICE

---

Do not place both regular and deduplication clients in the same group.

---

#### Procedure

1. Select the clients to be moved.
2. Drag the clients to another group.

## Estimating save set sizes of a backup group

You can estimate the size of the save sets that will be produced in a backup group before you run the backup.

#### Procedure

1. From the **Administration** window, click **Configuration**.
2. In the expanded left pane, select **Groups**.
3. Select the group to edit.
4. Select the **Advanced** tab.
5. In the **Option** attribute, select **Estimate, No Save, and Verbose**.

---

#### Note

Selecting the Estimate, No Save, and Verbose options produces an estimate that shows all paths and filenames that will be saved in the backup group. Selecting the Estimate and Verbose options produces a detailed estimate and performs the save in a single operation. Selecting only the Estimate option (without the No Save or Verbose option) results in a save operation without an estimate.

6. Click **OK**.

#### Results

To see the estimated save set sizes, open the daemon log file located in the NetWorker\_install\_dir\logs directory.

## Backup status reports

When the backup completes, several types of backup status reports are generated.

Information about the status of backed-up groups is also written to the savegrp log file, which is located in the NetWorker\_install\_dir\logs directory.

## Bootstrap report generation

When the backup group includes the NetWorker server, or if the server is not in an active group, the server generates a special save set called the bootstrap, which includes the media database and configuration files. In both of these cases, a bootstrap email

(default) or printout is generated whether the scheduled backup is initiated automatically or manually. The bootstrap information is essential for recovery from a disaster. For information on how the bootstrap is used during a disaster recovery operation, refer to the NetWorker SolVe Desktop.

#### **Note**

If the NetWorker server is not a member of an active group, the bootstrap is created when any group backup is run, even if the group has a level of SKIP. However, in this case the bootstrap will be created only once every 24 hours, regardless of how many groups run during that period. If you would like to create bootstraps for every group backup, you should include the server in the group with a very small save set (such as /etc/hosts).

---

By default, the bootstrap reports are generated and sent as an email to the default email recipient, either the administrator or root. To change the email recipient, open the Bootstrap notification and configure a new email recipient.

#### **Note**

Users can also choose to get the reports printed through the default printer configured for the NetWorker server. To change the default printer, edit the Printer attribute in the Group resource.

---

If you configure the bootstrap notification for email (default option) and do not configure an email recipient, then the bootstrap reports are lost. However, when an email recipient is later configured, the bootstrap reports are generated the next time as part of the savegrp operation and the previous reports are also sent to the email recipient along with the current report.

If you configure the bootstrap notification to the printer (not the default configuration) and the bootstrap report fails for any reason, then the contents can be viewed in the savegrp.log file, which is located in the <install\_dir>\logs directory, or the savegrp report.

## Open file backups

Open files are a problem that all data backup applications must solve. Open files that are not backed up properly represent a potential data loss. They might be skipped, improperly backed up, or locked.

NetWorker can open two different types of files. Those that are owned by the operating system and those that are owned by a specific application.

### Opening files owned by the operating system

Most open files that are owned by the operating system can be backed up. However, some applications can apply operating system locks to open files. These locks prevent other applications, such as NetWorker software, from writing to or reading from the open file.

The NetWorker software normally skips locked files and returns the message:

```
save: file_name cannot open
```

Additionally, the operating system might return a permission denied error.

To back up locked open files, close any open files. However in most cases, this is impractical. To automate this process, create a pre- and postprocessing backup command that shuts down specific applications, backs up the open files, and then

restarts any applications after the backup finishes. Also use Open File Manager to back up open files.

## Opening files owned by a specific application

The NetWorker software by itself cannot normally back up an open file that belongs to a specific application, like a database.

To back up these open files, use a NetWorker Module. For example, use the NetWorker Module for SAP to back up open files in an Oracle database.

## Backing up files that change during backup

If a file changes during a backup, the NetWorker software displays the following message in the Groups tab of the Monitoring option:

```
warning: file_name changed during save
```

To ensure that the changed file is backed up, do either of the following:

- Restart the backup group.
- Perform a manual backup.

---

### Note

NetWorker Modules can back up these types of files correctly if they are files related to the database the module is backing up.

## Open file backup with VSS

In NetWorker releases 7.6 and later, the software takes advantage of VSS technology to create snapshot backups of volumes and exact copies of files, including all open files. In this way, files that changed during the backup process are copied correctly.

## Schedules

Each Client resource is backed up according to a schedule. A Client resource's backup schedule tells the NetWorker server what level of backup (for example, full, incremental, or synthetic full) to perform on a given day. For instance, on Fridays it might perform a full backup on a Client resource and the rest of the week perform incremental backups. The time of day the backup begins is determined by the group to which the Client resource is associated.

Schedules can be simple or complex, depending on the needs of the environment. All Client resources can share the same schedule, or each can have a unique schedule.

The type and scope of the backup is determined by the specified backup level. The level can be set to back up a client's entire file system, or only data that has changed since the last full backup.

## Schedules for Avamar deduplication clients

Backups must be scheduled to avoid the Avamar node's read-only periods when such cron jobs as checkpoint and garbage-collection are run. The Avamar server documentation provides more information.

The *EMC NetWorker Avamar Integration Guide* provides backup level and schedule information that is specific to Avamar clients.

## Preconfigured NetWorker schedules

The NetWorker software ships with preconfigured schedules. If these schedules meet backup requirements, use them as is. Otherwise, create new schedules to accommodate any site-specific needs.

Preconfigured schedules cannot be deleted. Preconfigured schedules that contain "overrides" (indicated by an asterisk next to a backup level in the schedule's calendar) cannot be modified. All other preconfigured schedules can be modified.

The following table describes the preconfigured schedules.

**Table 34** Preconfigured NetWorker schedules

Schedule name	NetWorker backup operation
Default	Completes a full backup every Sunday, incremental backups on all other days.
Full Every Friday	Completes a full backup every Friday, incremental backups on all other days.
Full on First Friday of Month	Completes a full backup on the first Friday of the month, incremental backups on all other days. This schedule cannot be modified.
Full on First of Month	Completes a full backup on the first calendar day of the month, incremental backups on all other days.
Quarterly	Completes a full backup on the first day of a quarter. Performs a level 5 backup on the first day of the other months in the quarter. Every seven days, a level 7 backup occurs. Incremental backups are performed on all other days. This schedule cannot be modified.
Incremental and Synthetic Full 1st Friday of Month	Completes an incremental backup prior to performing a Synthetic Full backup on the first Friday of every month. Completes incremental backups on all other days. This schedule cannot be modified.
Incremental and Synthetic Full Every Friday	Completes an incremental backup prior to performing a Synthetic Full backup on every Friday. Completes incremental backups on all other days. This schedule cannot be modified.
Incremental and Synthetic Full 1st of Month	Completes an incremental backup prior to performing a Synthetic Full backup on the first calendar day of the month. Completes incremental backups on all other days. This schedule cannot be modified.

**Table 34** Preconfigured NetWorker schedules (continued)

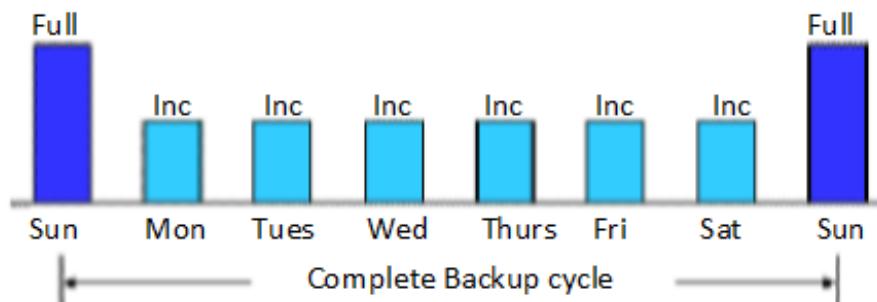
Schedule name	NetWorker backup operation
Incremental and Synthetic Full Quarterly	Completes an incremental backup prior to performing a Synthetic Full backup on the first day of each quarter. Completes incremental backups on all other days. This schedule cannot be modified.

## Backup cycles

The period of time from one full backup to the next full backup is called a backup cycle. The following examples demonstrate how to use schedules for different backup cycles and client backup needs.

### Weekly backup cycle example

The following figure illustrates a weekly backup cycle. In this example, a full backup is performed on a client each Sunday, and incremental (Inc) backups are performed on the other days of the week.

**Figure 18** Weekly backup cycle

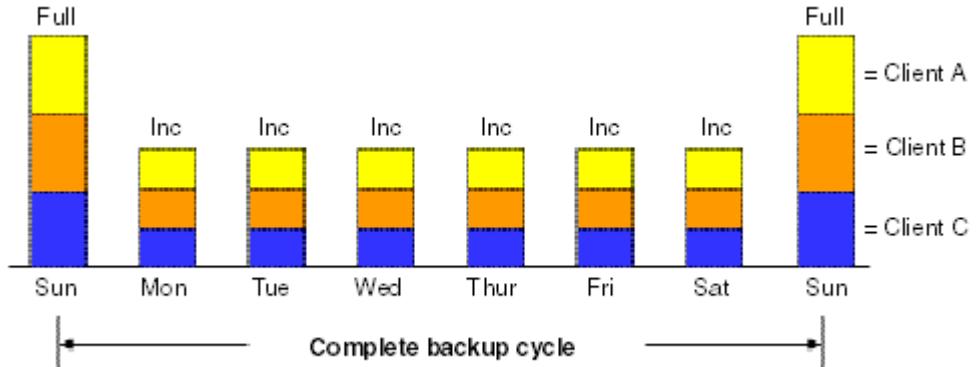
Use backup schedules to balance and stagger the load on a NetWorker server. Depending on the size of a network, you could apply the same schedule to all clients. For example, if no one works over the weekend and you want to run full backups during this time, you could apply the Default schedule to all of the clients.

The Default schedule tells the NetWorker server to perform full backups on Sunday, and incremental backups the rest of the week.

## Default schedule for multiple clients example

The following figure illustrates how the Default schedule works for three clients.

**Figure 19** Default schedule for multiple clients



### NOTICE

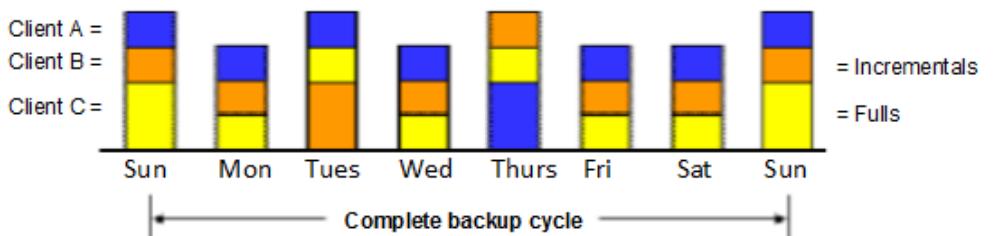
If you have a short backup window period and need to create a full backup, you can use the synthetic full backup.

Since full backups transfer large amounts of data and typically take longer than other backup levels, you might want to stagger them throughout the week. For example, you could apply a schedule that performs a full backup for Client A on Thursday, a second schedule that performs a full backup for Client B on Tuesday, and a third schedule that performs a full backup for Client C on Sunday.

## Staggered weekly schedules for multiple clients example

The following figure illustrates how to use a staggered backup schedule for multiple clients.

**Figure 20** Staggered weekly schedules for multiple clients

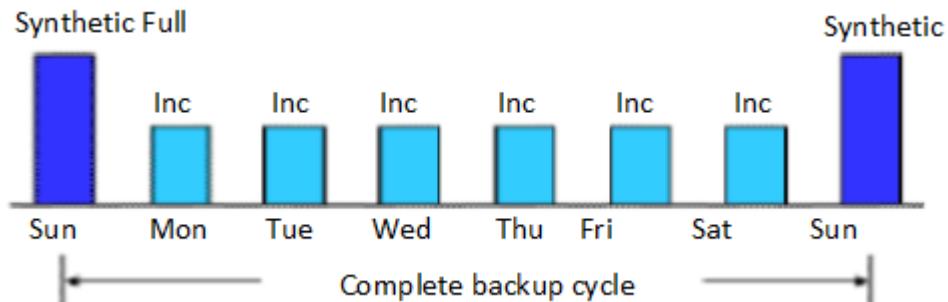


By balancing and staggering the load, and using different start times for different groups of clients, you can increase the efficiency of a NetWorker server.

## Weekly synthetic full backup cycle to reduce backup window example

The following figure illustrates a weekly full synthetic backup cycle. In this example, a synthetic full backup is performed on a client each Sunday, and incremental backups are performed on the other days of the week.

**Figure 21** Weekly synthetic full backup cycle to reduce backup window



## Considerations for scheduling and planning

Deciding which schedules are most appropriate for an environment requires planning.

When you create backup schedules, consider:

- How much data do you have to back up?
- How many backup media volumes do you plan to use?
- How much time do you have to complete a backup?
- Does it matter how many volumes are required to recover from a disaster, such as a disk crash?

Additionally, determine a policy for recovering files. For example, if users expect to be able to recover any version of a lost file that was backed up during a three-month period (that is, the retention policy is three months), you need to maintain all of the backup volumes for a three-month period. However, if users expect to be able to recover data from only the last month, you will not need to maintain as many volumes.

The browse and retention policies associated with each client determine the length of time that data is available for recovery by the NetWorker server.

### NOTICE

If you have a short backup window period and need to create a full backup, you can use the synthetic full backup.

## Scheduling large client file systems

At a moderate backup rate of 400 KB per second, a full backup for a client with 10 GB of data takes about seven hours to complete. Consequently, it might not be convenient to perform a scheduled, full backup for client save sets as large as this because of the amount of time required.

When scheduling large client file systems, consider the following:

- Schedule the client's disk volumes for backup at different times by separating them into different backup groups. When you split one client's save sets into multiple backup groups, you back up all the client's files, but not all at once. It is less time-consuming than a full backup of all the local data at one time.

- To back up the client's file systems individually, add and configure the same client several times by addressing the different file systems in the Client resource. For example, configure the first Client resource to back up one file system () with a single backup schedule in one group. Then, configure the second Client resource to back up another file system () with a second backup schedule in another group.

**NOTICE**

When you create separate backup schedules and explicitly list save sets, any files or file systems not included in that list are omitted from backup. This includes any new disk volumes that are added to the system. To avoid this risk, type the value All in the Save Set attribute.

## Key components of a schedule

The following table describes the key components of a Schedule resource.

**Table 35** Key components of a schedule

Attribute	Description
Name	The name assigned to a customized schedule that appears in the Client resource as an attribute, and can be applied to a client/save set. Assign a simple, descriptive name such as Monday Full.
Period	Determines how often a full backup is to run. Set the schedule to apply to either a weekly or a monthly period. When you select Week and set up a schedule, the backup level full is applied to the same day of the week for all weeks in the calendar year. For example, full backups every Sunday. Week is the default setting. When you select Month and set up a schedule, the backup level full is applied to the same day of the month for all months in the calendar year. For example, full backups on the fifteenth of each month.
Calendar	Displays the days of the month and the backup level scheduled for each day. In addition to full and incremental backups, you can set intermediate backup levels. You can include one or more of these levels in a backup schedule: <ul style="list-style-type: none"> <li>Full</li> <li>Incremental</li> <li>Level (1 – 9)</li> <li>Synthetic Full+Incr</li> <li>Skip</li> </ul> The Override Levels option allows you to override an existing backup level for a specific day. For example, you might not want a full backup to run on a holiday. You can override the schedule so the full backup runs on the day before or the day after the holiday. An asterisk next to a backup level indicates that an override has been set for that day. If you override backup levels by using the nsradmin command line program, you can also specify relative date values such as full first friday every 2 week. The nsr_schedule man page or the <i>EMC NetWorker Command Reference Guide</i> contains more information about overriding backup levels.

**NOTICE**

The Force Incremental attribute in the backup group determines the level used by the NetWorker server when there is more than one backup per day. The default value for this attribute is Yes, which means that an incremental backup will occur if the group is run more than once a day. To perform more than one full or level backup per day, set this attribute to No.

---

## Working with schedules

This section provides information on how to create, edit, delete, and copy schedules.

### Creating a schedule for backups

A schedule can be applied to each client backup. Use the following procedure to create a schedule for backups.

#### Procedure

1. From the **Administration** window, click **Configuration**.
2. In the expanded left pane, select **Schedules**.
3. From the **File** menu, select **New**.
4. In the **Name** attribute, type a name for the schedule.
5. From the **Period** attribute, select **Week or Month**.
  - Select **Week** to create a weekly backup schedule. For example, if a full backup for a Friday is selected, every Friday will have a full backup.
  - Select **Month** to create a monthly schedule. For example, if a full backup for the first of the month is selected, every month will have a full backup on the first of the month.
6. Select a backup level for each day in the weekly or monthly period:
  - a. Select a day.
  - b. Right-click and from the **Set Level** menu, select a backup level.
7. If required, select an override backup level for any day. An override occurs once only for the selected day:
  - a. Select a day.
  - b. Right-click and from the **Override Level** menu, select a backup level.
8. Click **OK**.

### Editing a schedule

#### Procedure

1. From the **Administration** window, click **Configuration**.
2. In the expanded left pane, select **Schedules**.
3. In the right pane, select the schedule to edit.
4. From the **File** menu, select **Properties**.
5. Edit the attributes and click **OK**.

## Deleting a schedule

You cannot delete preconfigured schedules or schedules that are currently selected in a client's Schedule attribute.

### Procedure

1. From the **Administration** window, click **Configuration**.
2. In the expanded left pane, select **Schedules**.
3. In the right pane, select the schedule to delete.
4. From the **File** menu, select **Delete**.
5. When prompted, click **OK** to confirm the deletion.

## Copying a schedule

### Procedure

1. From the **Administration** window, click **Configuration**.
2. In the expanded left pane, select **Schedules**.
3. In the right pane, right-click the schedule you want to copy and select **Copy**. The **Create Schedule** dialog box appears with the same information as the schedule that was copied, except for the Name attribute.
4. In the **Name** attribute, type a name for the new schedule.
5. Edit the attributes and click **OK**.

## Overriding a client's regular backup schedule

You can set the Schedule and Level attributes in the group to override a client's regular backup schedule.

For example, one evening you can run a full backup on all the clients in a group, regardless of the clients' regular backup schedules. The value specified in the group's Level attribute overrides the backup level setting for every client in the group.

Alternatively, you can have a group of clients follow the same backup schedule instead of each client's individual schedule. You could assign a group of clients to follow the default schedule (full every Sunday) regardless of each client's individual schedule. If you leave the group's Level and Schedule attributes blank (the default setting), clients follow the backup schedule assigned in the Client resource.

## Disabling or enabling a client backup schedule

By default, the schedule assigned to the backup client is enabled.

### Procedure

1. Open the **Client** resource whose scheduled backups are to be disabled. [Editing a client on page 528](#) provides more information.
2. Clear the **Scheduled Backup** attribute and click **OK**.

## Backup levels

Because it may not be practical or efficient to run full backups every day, you can specify the level of the backup to be performed during scheduled backups.

By limiting the frequency of full backup, you help maintain server efficiency, while still ensuring that data is protected. Different backup levels enable you to trade off the

number of volumes and amount of time required to complete a backup to recover from a disk crash.

The following figure describes the five kinds of backup levels:

**Table 36** Backup levels

Backup Level	Function
Full	Backs up all files, regardless of whether or not they have changed.
Level [1 – 9]	<p>Backs up files that have changed since the last backup with a lower-numbered backup level. For example:</p> <ul style="list-style-type: none"> <li>• A level 1 backup backs up all files that have changed since the most recent full backup (considered a level zero).</li> <li>• A level 3 backup backs up all files that have changed since the most recent backup at level 2, level 1, or full. For example, if the most recent backup was at level full, then a level 3 backup will back up all files that changed since the full backup. However, if the most recent backup was at level 2, then a level 3 backup will back up only those files changed since the level 2 backup.</li> <li>• A level 9 backup backs up all the files that have changed since the most recent backup of any level except level 9.</li> </ul> <p>The NetWorker software ignores any incremental-level backups when determining what files should be backed up.</p>
Incremental	Backs up files that have changed since the last backup, regardless of level.
Synthetic Full	Backs up all data that has changed since last full backup and subsequent incrementals to create a synthetic full backup.
Synthetic Full +Incr	<p>Perform an incremental backup and a synthetic full backup on the same day in the same group.</p> <p>Use this level when synthetic full backups fail because the incremental backup chain is broken. This level triggers an incremental to be created before the synthetic full backup. This mends the broken chain of incremental backups.</p>
Skip	Skips the scheduled backup. For example, you can skip a backup on a holiday if no one will be available to change or add more media volumes.

#### Note

Information on the special nature of deduplication backups is available in the *EMC NetWorker Avamar Integration Guide* and the *EMC NetWorker Data Domain Deduplication Devices Integration Guide*.

## How NetWorker backup levels work

Backup levels work in conjunction with a client's backup schedule. The way you define the backup levels directly affects how long a recovery from a disk crash takes and how many backup volumes you need.

Planning level backups helps to minimize the number of volumes used. The fewer volumes required to recover from a disk crash, the less time spent restoring the disk.

You can also reduce the size and time it takes to back up data by using directives. For example, use a directive to skip certain files or file systems when performing a backup.

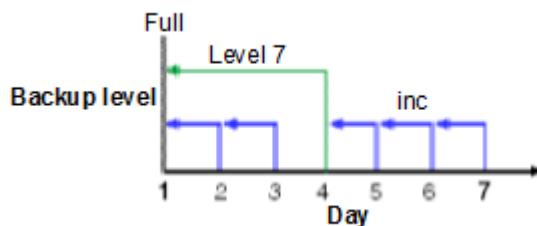
The following examples illustrates how the backup levels affect the requirements for data recovery.

In the following figure, a full backup runs on October 1. On October 2, an incremental backup saves everything that changed since the full backup. On October 3, another incremental backup backs up everything that changed since October 2. Then, on October 4, a level 7 backup backs up everything that changed since the full backup on October 1.

To fully recover from a disk crash on October 4, you need the data from the full backup from October 1 and the new level 7 backup. You no longer need the data from October 2 and 3, because the level 7 volume includes that information.

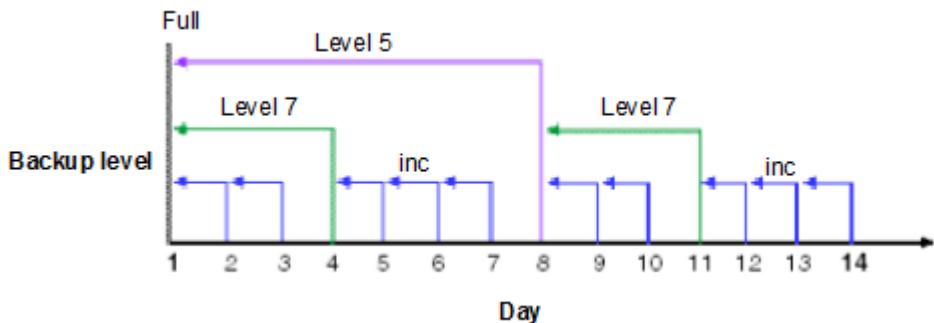
Also, incremental backups on October 5, 6, and 7 back up everything that has changed since the level 7 backup on October 4.

**Figure 22** Backups for October 1 through October 7



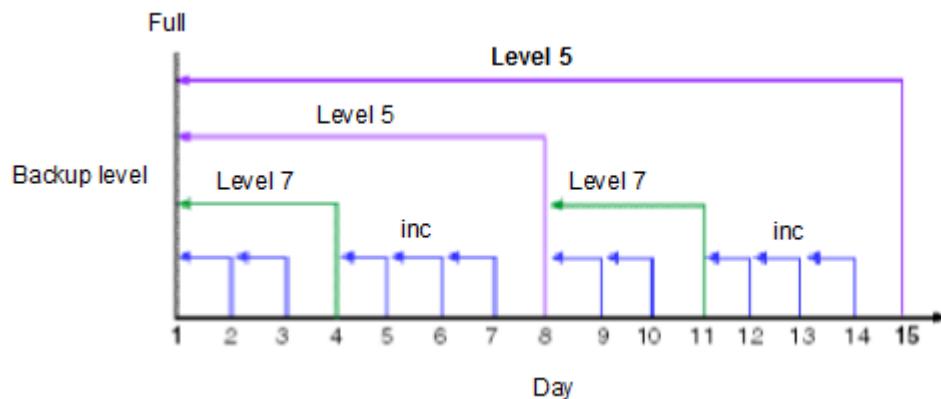
The following figure continues the previous figure by showing a level 5 backup on October 8, which backs up everything that changed since the full backup on October 1. To fully recover from a disk crash on October 8, you only need the data from October 1 and the new level 5 volume. You no longer need the data from the level 7 backup on October 4 (or the subsequent incremental backups performed on October 5, 6, and 7) because the new level 5 backup includes that data.

**Figure 23** Backups for October 1 through October 14



Also, a level 7 backup on October 11 backs up all of the data that changed since the last lower-numbered backup (in this case, the level 5 backup on October 8). To recover from a disk crash on October 11, you need three volumes: the full volume from October 1, the level 5 volume from October 8, and the new level 7 volume.

The following figure continues the example by showing a level 5 backup on October 15, which backs up all of the data that changed since the last lower-numbered backup. Because no backup lower than level 5 has been performed since the full backup on October 1, this level 5 backs up all of the data that changed since the full backup. Therefore, to recover from a disk crash on October 15, you only need the data from the full backup on October 1 and the new level 5 backup.

**Figure 24** Backups for October 1 through October 15

## The NetWorker server and backup levels

A backup schedule defines what level backup to perform on a given day. You can apply one or more backup levels to customize a backup schedule. To use backup levels in a customized schedule, consider these issues to help you decide what best suits your environment.

- Full backups generally take more time to complete than incremental backups. The exception to this is the full backup of deduplication clients. With deduplication, only the initial full backup takes longer. Thereafter, every full backup captures only the exact bits that have changed. This allows the subsequent full backups to be significantly smaller.
- If you have only one stand-alone storage device and the full backup does not fit on a single piece of media, an operator must be available to monitor the backup and change the media.
- Full backups cause the online indexes to grow more rapidly than incremental or level backups.
- Level backups serve as checkpoints in schedules because they collect all the files that have changed over several days, or even weeks, into a single backup session.
- Synthetic Full backups provide the same benefits at the same cost as do full backups. The difference is that synthetic full backups are less taxing on the network and client because a new full backup is created from a previously created full or synthetic full backup and subsequent incremental backups.

The following table lists advantages and disadvantages of each backup level.

**Table 37** Advantages and disadvantages of backup levels

Backup level	Advantages	Disadvantages
Full	<ul style="list-style-type: none"> <li>• Faster recovery</li> </ul>	<ul style="list-style-type: none"> <li>• Slow backup</li> <li>• High server load</li> <li>• High load on client and network</li> <li>• Uses more volume space</li> </ul>
Level	<ul style="list-style-type: none"> <li>• Faster than performing a full backup</li> <li>• Low load on server</li> </ul>	<ul style="list-style-type: none"> <li>• Slow recovery</li> </ul>

**Table 37** Advantages and disadvantages of backup levels (continued)

Backup level	Advantages	Disadvantages
	<ul style="list-style-type: none"> <li>• Uses least volume space</li> </ul>	<ul style="list-style-type: none"> <li>• Data can spread across multiple volumes</li> </ul>
Incremental	<ul style="list-style-type: none"> <li>• Faster than performing a full backup</li> <li>• Low load on server</li> <li>• Uses less volume space than a full backup</li> </ul>	<ul style="list-style-type: none"> <li>• Slow recovery</li> <li>• Data can spread across multiple volumes</li> </ul>
Synthetic Full	<ul style="list-style-type: none"> <li>• Faster than performing a full backup</li> <li>• Faster recovery</li> <li>• Low load on server, client and network</li> <li>• Requires less volumes for recover</li> </ul>	<ul style="list-style-type: none"> <li>• High load on storage node</li> <li>• Requires at least two volume drives</li> <li>• Uses most volume space</li> </ul>

## Online indexes and backup levels

The NetWorker server backs up the online indexes (client file index and media database) differently than regular files and other data.

Knowing how the online indexes are backed up is particularly important during disaster recoveries.

The online indexes are backed up in the following way:

- The client file index for a NetWorker client is backed up every time the client is backed up. When a client's backup level is incremental, the backup of its client file index is at level 9. For a synthetic full backup, the backups of the indexes are level 9. The NetWorker server does not perform a level 1 backup for this data. The files associated with the client file index of a NetWorker client reside on the NetWorker server. So, when a client is backed up, its client file index is also backed up on the NetWorker server.
- The client file index for the NetWorker server client is backed up every time the NetWorker server is backed up. When the server's backup level is incremental, the backup of its client file index is at level 9. For a synthetic full backup, the backup of the index is level 9. The NetWorker server does not perform a level 1 backup for this data.

For example:

- If the NetWorker server is backed up at the level full, the backup levels of the NetWorker server's client file index, the media database, and the resource database are also full.
- If the NetWorker server's backup is a level 5, the backup of the server's client file index is also a level 5.
- The media database and the resource database are backed up whenever the NetWorker server is backed up, or after every scheduled backup if the server is not in an active group. determine what level the MM and res are run at

The following table compares the level at which the NetWorker server backs up regular files and the online indexes.

**Table 38** Regular file and index backup levels

<b>Regular files</b>	<b>Online indexes do we need to differentiate between CFI, MM and res</b>
Full	Full
Level 2 – 9	Level 2 – 9
Incremental	Level 9
Manual (using the User program)	Not saved
Synthetic full	Level 9

Disabling the Windows Archive attribute this may need to be updated as not applicable for windows 2008

The NetWorker software uses the Windows file Archive attribute to help determine if the file should be backed up. The NetWorker software backs up a file if the Archive attribute is enabled.

- After backing up the file, the NetWorker software turns off the Archive attribute.
- After restoring the file, the NetWorker software turns on the Archive attribute.

#### Procedure

1. Set the environment variable *NSR\_AVOID\_ARCHIVE* to a value of **Yes**.

To set this as a system environment variable, use the Control Panel's System applet. If this variable is used, NetWorker determines a file's need to be backed up based on the traditional save criteria of modification time.

2. Log off, reboot, or restart the **NetWorker Remote Exec Service** to make Windows aware of the system environment variable change.

# CHAPTER 9

## Directives

This chapter contains the following topics:

- [Directives overview](#)..... 270
- [Types of local and global directives](#)..... 270
- [Creating a global directive resource](#)..... 270
- [Editing a global directive resource](#)..... 271
- [Deleting a global directive resource](#)..... 271
- [Copying a global directive resource](#)..... 271
- [Example directives](#)..... 272
- [Local directives within the NetWorker User program](#)..... 273
- [Preconfigured global directive resources](#)..... 274
- [Format of directive statements](#)..... 276
- [Application Specific Modules \(ASMs\)](#)..... 278

## Directives overview

Directives are resources that contain special instructions that control how the NetWorker server processes files and directories during backup and recovery. NetWorker administrators can create directives to customize the NetWorker software to your specific needs, maximize the efficiency of backups, and apply special handling to individual files or directories.

**NOTICE**

Do not leave blank lines in directive scripts.

---

## Types of local and global directives

There are three types of directives.

**NOTICE**

If you are using the Windows BMR feature, employ user defined directives with caution. Using such directives in directories where system state files reside will lead to an incomplete BMR backup image and potentially render your BMR backup image unusable. If you create user defined directives, test your BMR backup image to ensure that you can recover your Windows system state correctly.

---

### Global directives

Administrators can create global directives by using the NetWorker Administration window. These directives are stored as resources on the NetWorker server, and can be selectively applied to individual clients by using the Directive attribute of the Client resource.

### NetWorker User local directives (Windows only)

On clients that run Microsoft Windows, users with local Windows Administrator or Backup Operator privileges can create local directives by using the NetWorker User program. These directives are stored on the client in a file named networkr.cfg, and are applied throughout the client's file systems during scheduled backups (or save operations that do not include the -i option).

### Local directive files

Users can create local directive files named nsr.dir (Windows) or .nsr (UNIX) anywhere on a client file system that they have permission to create files. These directives apply only to the immediate data within the path where the directive file is located.

## Creating a global directive resource

[Format of directive statements on page 276](#) provides instructions on the syntax to use when creating directives.

#### Procedure

1. From the **Administration** window, click **Configuration**.
2. In the expanded left pane, select **Directives**.
3. From the **File** menu, select **New**.
4. In the **Name** attribute, type a name for the new directive.
5. In the **Comment** attribute, type a description of the directive.
6. In the **Directive** attribute, type one or more directives.
7. Click **OK**.

#### Results

The directive can now be applied to a NetWorker Client resource.

## Editing a global directive resource

A directive name cannot be changed, the directive must be deleted and a new one created with a new name.

#### Procedure

1. From the **Administration** window, click **Configuration**.
2. In the expanded left pane, select **Directives**.
3. In the right pane, select the directive.
4. From the **File** menu, select **Properties**.
5. In the **Directive** attribute, modify the directive as necessary and then click **OK**.

## Deleting a global directive resource

You cannot delete preconfigured directives or any directives currently applied to a Client resource.

#### Procedure

1. From the **Administration** window, click **Configuration**.
2. In the expanded left pane, select **Directives**.
3. In the right pane, select the directive to delete.
4. From the **File** menu, select **Delete**.
5. Click **Yes** to confirm the deletion.

## Copying a global directive resource

#### Procedure

1. From the **Administration** window, click **Configuration**.
2. In the expanded left pane, select **Directives**.
3. In the right pane, select the directive to copy.
4. From the **Edit** menu, select **Copy**.

A copy of the directive is created.

5. In the **Name** attribute specify a name for the directive.
6. In **Directive** attribute, modify the directive as necessary and then click **OK**.

## Example directives

This section contains some basic examples of global and local directives, and describes how to apply them to NetWorker clients.

### Applying a global directive example

This example shows how to use a global directive to skip all \*.tmp files in a particular directory for a particular NetWorker client.

#### Procedure

1. Create a global directive by using the appropriate format:
  - On Windows, skip all \*.tmp files in the C:\mydir directory:  
 <<"C:\MYDIR">>  
 skip: \*.tmp
  - On UNIX, skip all \*.tmp files in the /mydir directory:  
 <</mydir>>  
 skip: \*.tmp
2. Apply the directive to the appropriate NetWorker Client resource:
  - a. From the **Administration** window, click **Configuration**.
  - b. In the left pane, click **Clients**.
  - c. In the right pane, select a client.
  - d. From the **File** menu, select **Properties**.
  - e. From the **Directives** attribute list, select a directive and then click **OK**.

#### Results

When a scheduled backup is performed on the NetWorker client, all files that match the \*.tmp pattern in the specified directories will be skipped.

### Applying a NetWorker User program local directive example (Windows only)

This example shows how to use a Windows local directive to skip all \*.tmp files in the C:\mydir directory on a particular NetWorker client.

Using the NetWorker User program, create a local directive. The directive is saved in the networkr.cfg file in this format:

```
<<"C:\mydir">>
skip: *.tmp
```

When a scheduled backup is performed on the NetWorker client, all files that match the \*.tmp pattern in the C:\mydir directory will be skipped.

### Applying a local file directive example

This example shows how to use a local file directive to skip all \*.tmp files in a particular directory for a particular NetWorker client. When a scheduled backup is performed on the

NetWorker client, all files that match the \*.tmp pattern in the specified directory will be skipped.

On Windows, skip all \*.tmp files in the C:\mydir directory:

1. Use a text editor to create a file named nsr.dir and type this directive in the file:

```
skip: *.tmp
```

2. Place the nsr.dir file in the C:\mydir directory on the NetWorker client.

#### Note

To create directive files on a client that is running Microsoft Windows, an authenticated user must have the appropriate permissions to create files either within the root of a volume, or in a folder within the volume.

On UNIX, skip all \*.tmp files in the /mydir directory:

1. Use a text editor to create a file named .nsr and type this directive in the file:

```
skip: *.tmp
```

2. Place the .nsr file in the /mydir directory on the NetWorker client.

## Order of precedence of global and local directives

If there is a conflict between directives, global directives are enforced over local directives. And on Windows hosts, NetWorker User program local directives are enforced over local directive files (nsr.dir files).

## Local directives within the NetWorker User program

On Windows, users can create local directives with the NetWorker User program. These directives are saved in a file named networkr.cfg.

When you perform a manual backup from the NetWorker User program, only local directives that were created with the NetWorker User program are enforced. Global directives and local directive files (nsr.dir files) are not enforced. However, all local directives are enforced when the NetWorker save command without the -i option is run at the command prompt.

NetWorker User program local directives are also enforced during scheduled backups and archive operations.

## Setting up a NetWorker User program local directive

### Procedure

1. Log in to the client computer as a member of either the local **Windows Administrators** or **Backup Operators** **Window > s** security group.
2. Start the **NetWorker > User Program**.
3. From the **Options** menu, select **Local Backup Directives**.
4. Set the local directive for each data item. You can clear data items in order to exclude them from scheduled backups, and select items for password-protection, encryption, and compression. This applies for both manual and scheduled saves.

**Note**

If password-protection or encryption is selected, the password must be specified first.

5. From the **File** menu, select **Save Backup Directives** to save changes.

Depending on user privileges and OS version, the User program creates networkr.cfg in one of these locations:

- If you are logged on with local Windows Administrator or Backup Operator privileges, networkr.cfg is created in the root of the system volume (usually C:\).
- If you are not logged on with local Windows Administrator or Backup Operator privileges, NETWORKR.CFG is created in %SystemDrive%\Documents and Settings\User\_name\Application Data\EMC NetWorker

**Note**

The Application Data directories are hidden by default. To view these directories by using Windows Explorer, select **Tools > Folder Options**. On the View tab of the View Options dialog box, select the Show hidden files and folders option.

## Preconfigured global directive resources

The NetWorker software comes with a number of preconfigured global Directive resources. All preconfigured Directive resources can be modified, but they cannot be deleted.

The following table lists the preconfigured directives and their descriptions.

**Table 39** Preconfigured directives

Directive resource	Description
AES	Encrypts backup data with the aes ASM, which provides 256-bit data encryption.
DOS standard	Legacy resource that is used to back up Microsoft Windows 95 and Windows 98 clients. By default, this resource has no directives.
DOS with compression	Legacy resource that is used to back up and compress Microsoft Windows 95 and Windows 98 clients. Applies the compressasm ASM to all files.
Mac OS with compression	Contains the same set of directives as the Mac OS standard directive, along with applying the compressasm ASM to specific directories.
Mac OS standard	Contains a set of directives used to back up standard Mac OS clients. Applies these ASMs: <ul style="list-style-type: none"> <li>• The skip ASM is applied to these files and directories:               <ul style="list-style-type: none"> <li>/Desktop DB</li> <li>/Desktop DF</li> <li>/cores</li> <li>/VM_Storage</li> <li>/TheVolumeSettingsFolder</li> <li>/private/var/db/netinfo</li> </ul> </li> </ul>

**Table 39** Preconfigured directives (continued)

Directive resource	Description
	<p>/private/var/db/openldap      /private/tmp      /.Spotlight-V100      /.hotfiles.btree</p> <ul style="list-style-type: none"> <li>• The allow save environment keyword is applied to the /nsr directory to ensure that local directives in /nsr and subsequent subdirectories are applied.</li> <li>• The logasm ASM is applied to the /nsr/logs and /var directories.</li> <li>• The swapasm ASM is applied to the /private/var/vm</li> </ul>
NetWare standard	Is used to back up NetWare clients. By default, this resource has no directives.
NetWare with compression	Is used to back up and compress NetWare clients. Applies the compressasm ASM to all files.
NT standard	Is used to back up Windows clients. By default, this resource has no directives.
NT with compression	Used to back up and compress Windows clients. It applies the compressasm ASM to all files.
UNIX standard	<p>Contains a set of directives used to back up standard UNIX clients. Applies these ASMs:</p> <ul style="list-style-type: none"> <li>• The skip ASM is applied to the tmp_mnt directory.</li> <li>• The skip ASM is applied to core files on the file system.</li> <li>• The allow save environment keyword is applied to the /nsr directory to ensure that local directives in /nsr and subsequent subdirectories are applied.</li> <li>• The skip ASM is applied to the /tmp directory.</li> <li>• The swapasm ASM is applied to the /export/swap directory. If swap files are located in a different directory, modify this directive to use the appropriate directory.</li> <li>• The logasm ASM is applied to the /nsr/logs, /var, /usr/adm, and /usr/spool directories. You can apply this ASM to other directories as well.</li> <li>• The mailasm ASM is applied to the /usr/spool/mail and /usr/mail directories. If email files are located in different directories, modify these directives to use the appropriate locations.</li> </ul>
UNIX with compression	Contains the same set of directives as the UNIX standard directive, along with applying the compressasm ASM to all files. This directive is only applied to save sets that contain directories. If the save set is defined by using a filename, this directive will not be applied.
VCB directives	<p>VCB directives are valid for backing up virtual machines using the VCB methodology. This directive is supported in the following scenarios:</p> <ul style="list-style-type: none"> <li>• When file level incremental backups are performed instead of FULL image level backups.</li> </ul>

**Table 39** Preconfigured directives (continued)

Directive resource	Description
	<ul style="list-style-type: none"> <li>When FULL file level or incremental file level backups are performed when the save set is ALLVMFS. The vcb directive skips the following files and folders:</li> <li>pagefile.sys</li> <li>hiberfil.sys (Hibernation file)</li> <li>WINDOWS\system folder</li> <li>WINDOWS\System32 folder</li> </ul>

## Format of directive statements

The format of a directive uses three primary types of statements:

- Directory specifications
- ASM specifications
- Save environment keywords

Any text after a hash (#) character is treated as a comment. More information about directive formats can also be found in the nsr and nsr\_directive pages of the *EMC NetWorker Command Reference Guide* or the UNIX man pages.

**NOTICE**

Do not leave blank lines in directive scripts.

## Directory specifications

Directory specifications indicate the highest-level directory to which these ASMs apply. Be aware of the following considerations when adding directory specifications:

- You cannot use wildcards in directory specifications.
- When multiple directory specifications are used, directives that follow a directory specification apply to that directory until the next directory specification.
- Mount points, including nested mount points, must have their own directory specification.
- For directives applied to clients on Windows systems, pathnames are not case-sensitive. If there is a colon (:) in the pathname, the entire path must be enclosed in quotation marks.

The format for a directory specification is:

```
<<directory>>
• On Windows:
<<"C:\BIN">>
asm
<<"C:\TEMP">>
asm
```

- On UNIX:
 

```
<<"/etc">>
asm
<<"/tmp">>
asm
```

## ASM specifications

ASMs specify the action to take on one or more files. The syntax for an ASM specification is:

[+]asm: argument

where:

- The optional plus sign (+) indicates that the directive applies to both the current directory and all subdirectories.
- asm is the name of the ASM to be executed
- argument is a list of names (files or directories) that are acted upon by the ASM. The argument can include multiple names, separated by spaces, and can also specify wildcards. The argument can contain names that are in the current directory only. Subdirectories cannot be specified in the argument.

If an ASM or argument name includes a space, enclose the name or argument in double quotes.

### Note

For directives applied to clients on Microsoft Windows systems, filenames are case-sensitive.

## Using wildcards in ASM specifications

Wildcards can be used in ASM specifications to replace a single character or string of characters. Standard shell command interpreter filematching patterns are supported.

On UNIX systems, when applying a directive to all files, including hidden files, use \*.\* (insert a space after the first asterisk).

## Save environment keywords

Save environment keywords are used to control how the current ASM and subsequent ASMs that apply to the current directory and subdirectories will be applied.

The following table lists the three save environment keywords.

**Table 40** Save environment keywords

Keyword	Instruction	Example
forget	Instructs the NetWorker server to no longer apply inherited directives (those directives that begin with a +).	To skip all *.o files in the directory G:\SRC, except those in the G:\SRC\SYS directory, type:  <pre>&lt;&lt;G:\SRC&gt;&gt; +skip: *.o &lt;&lt;G:\SRC\SYS&gt;&gt; forget</pre> This uses the skip ASM to instruct the NetWorker server to skip all files named *.o in the SRC directory and all

**Table 40** Save environment keywords (continued)

Keyword	Instruction	Example
		subdirectories. It then uses the forget keyword to instruct the server to not apply the skip ASM to the SYS subdirectory.  The forget keyword works only if the corresponding directories are also explicitly specified in the NetWorker client resource's Save Set attribute. In the previous example, both the G:\SRC and the G:\SRC\SYS directories must be explicitly specified on separate lines in the client's Save Set attribute.
ignore	Instructs the NetWorker server to ignore all directives applied to the subdirectories below the current directory.	To override any local directives set in users' home directories, type:  <<HOME>> ignore
allow	Used in subdirectories that currently have the ignore keyword applied to them, and overrides the ignore.	Building on the preceding example for the ignore keyword, to allow directives in the HOMEDOC directory to be applied, type:  <<HOME>> ignore <<HOMEDOC>> allow

## Application Specific Modules (ASMs)

Directives use Application Specific Modules (ASMs) to process files and directories. ASMs are programs that operate within the NetWorker environment to perform various tasks during backup and recovery. For example, the compressasm program instructs the NetWorker server to compress data during backup.

ASMs are specified in a directive and are then executed during the backup of client data. Directives can contain one or more ASMs. The following table describes the NetWorker ASMs.

**Table 41** NetWorker ASMs

ASM name	Description	Example
aes	Encrypts backup data when included in a global directive that is associated with a Client resource.	+aes: *
always	Always backs up the specified files, independent of the change time of the file, and ignores the scheduled level. This ASM can be used to ensure that important client files that change constantly are always fully backed up.	always: *.c

**Table 41** NetWorker ASMs (continued)

ASM name	Description	Example
compressasm	<p>Compresses files so that they use less network bandwidth and fewer volumes. This ASM does not compress directories. The amount of compression achieved is data-dependent. This ASM can use considerable CPU resources, so its benefits could be limited on low-powered systems.</p> <p>Some storage devices such as cloud devices and deduplication devices have their own encryption capabilities. If such a device is already set up to compress data, then using the compressasm will likely yield no added benefit. In fact, the additional compression may result in slightly more data being written to your device.</p> <p>Three types of compression are supported:</p> <ul style="list-style-type: none"> <li>• Default NetWorker compression</li> <li>• gzip compression</li> <li>• bzip2 compression</li> </ul>	<p>For default NetWorker compression, specify one of the following: +compressasm: . +compressasm -default: .</p> <p>For gzip compression, specify the -gzip argument with a compression level from 0 to 9. A value of 0 provides the least compression and 9 provides the most compression. If no level is specified, the default value is 6: +compressasm -gzip 3: .</p> <p>For bzip2 compression, specify the -bzip2 argument with a compression level from 0 to 250. A value of 0 provides the least compression and 250 provides the most compression. If no level is specified, the default value is 0: +compressasm -bzip2 250: .</p> <p>Added compression uses more CPU resources and therefore, could increase backup times.</p> <p>Both gzip and bzip2 compression cannot be used with the aes encryption ASM.</p>
holey	Handles holes or blocks of zeros when backing up files and preserves these holes during recovery. This ASM is normally applied automatically and does not need to be specified.	+holey: *
logasm	Instructs the NetWorker server to not generate errors when the files specified by this ASM are in use. This ASM is useful for files involved in logging, and other similar files that might change during a backup operation.	+logasm: *.log

**Table 41** NetWorker ASMs (continued)

ASM name	Description	Example
mailasm	Uses mail-style file locking and maintains the access time of a file, preserving "new mail has arrived" flag on most mail handlers.	+mailasm: *.mbx
mtimeasm	Backs up files by using the modification time, rather than the inode change time, to determine which files should be backed up. The modification time is the last time the file's contents were modified, while the inode change time is the last time the file's mode, owner, or link count was changed.	mtimeasm: *.log
nsrindexasm	Used to recover from NetWorker file index backups performed by NetWorker servers prior to release 6.0. During recovery from these older index backups, nsrindexasm is invoked automatically by nsrck and mmrecov.	Not applicable
nsrmfdbasm	Used to process the media database. Normally, nsrmfdbasm is invoked automatically by savegrp and mmrecov, and should not be used in NetWorker directives.	Not applicable
null	Does not back up the specified files, but does back up the directory containing the files so entries for the files get added to the online indexes. The NetWorker server uses this ASM to back up the online indexes during a scheduled backup.	+null: *.tmp
nullasm	Another name for the null ASM, used for backward compatibility.	See null.
posixcrcasm	Calculates a 32-bit cyclic redundancy check (CRC) for a file during backup. This CRC is stored along with the file and is verified when the file is restored. No verification occurs during the backup itself. With this ASM, it is possible to validate a file at restore time, but it does not provide a way to correct any detected errors.	posixcrcasm: *.*
rawasm	Specifies the back up of UNIX raw disk partitions. The /dev entries (block and character-special files) and their associated raw disk partition data is backed up. On some systems, /dev entries are symbolic links to device specific names. Unlike other ASMs, this ASM follows symlinks, allowing the shorter /dev name to be configured.	rawasm: /dev/oracle1
skip	Omits files and directories from the backup, and does not place the directory or filename in the online index. In the example given, all files and directories with the name temp will be omitted from the backup.	+skip: temp
swapasm	Does not back up actual file data, but re-creates a zero-filled file of the correct size on recovery. This ASM is used on systems where the swapping device	swapasm: compression.doc

**Table 41** NetWorker ASMs (continued)

ASM name	Description	Example
	is a swap file that must be recovered with the correct size, but the contents of the swap file are not important and do not need to be backed up or restored.	
xlateasm	Translates file data so that data backed up is not immediately recognizable.	xlateasm: *.*

## Precautions when using rawasm to back up UNIX raw partitions

One can specify the rawasm directive to back up raw disk partitions on UNIX. However, if the raw partition contains data managed by an active database management system (DBMS), ensure that the partition is offline and the database manager is shutdown. For greater flexibility when backing up partitions that contain data managed by a DBMS, use a NetWorker Module application.

Similarly, if rawasm is used to save a partition containing a UNIX file system, the file system must be unmounted or mounted read-only to obtain a consistent backup.

---

### Note

Do not specify the rawasm directive to backup or recover raw partitions on Windows.

---

## Using rawasm to recover a UNIX raw partition

When recovering data, rawasm requires that the file system node for the raw device exist prior to the recovery. This protects against the recovery of a /dev entry and the overwriting of data on a reconfigured disk. You can create the /dev entry, having it refer to a different raw partition, and force an overwrite if needed. If you create the /dev entry as a symbolic link, the data is recovered to the target of the symbolic link.

Recovery of a raw partition must occur on a system configured with the same disk environment and same size partitions as the system that performed the backup:

- If the new partition is smaller than the original partition, the recovery will not complete successfully.
- If the new partition is larger than the original partition the estimated size reported upon recovery is not accurate.

## File matching with multiple ASMs in a directive

When a file matches multiple ASMs in a directive, the action taken on the file depends on the order of the ASMs in the directive. For example, if these ASMs are listed in a directive:

+always: master.mdf master.ldf

+skip \*.mdf \*.ldf

Then the master.mdf and the master.ldf files will be backed up because the always ASM is processed first. All other files with a .mdf or .ldf extension will not be backed up.

However, if the order of the ASMs is reversed:

+skip \*.mdf \*.ldf

+always: master.mdf master.ldf

The master.mdf and the master.ldf files will not be backed up because the skip ASM is processed first.

---

**Note**

To simplify directives that include multiple potential matches for the same file, consider using save environment keywords.

---

# CHAPTER 10

## Sorting Backup Data

This chapter contains the following topics:

- [Media pools](#)..... 284
- [Label templates](#)..... 298

## Media pools

Backup data is sorted onto backup media volumes by using media pools and volume labels. A media [pool on page 760](#) is a specific collection of volumes to which the NetWorker server writes data. The server uses media pools to sort and store data. A volume is identified with a unique label based on configurable label templates.

Media pools act as filters that tell the server which backup volumes should receive specific data. The NetWorker server uses media pools in conjunction with label templates (if the Match Bar Code Labels attribute is not used for the library resource) to keep track of what data is on which specific volume.

---

**Note**

Media pools do not apply when deduplication is used.

---

## Using media pools

Each media pool configuration includes criteria that must be met in order for the data to be written to associated volumes.

When a scheduled backup occurs, the NetWorker server tries to match the save stream to a media pool configuration. If the save stream matches the criteria of a media pool configuration, it is directed to a labeled volume in the media pool. The server then checks if a correctly labeled volume for that media pool is mounted on a storage device:

- If a correctly labeled volume is mounted on a storage device, the NetWorker server writes data to the volume.
- If there is no correctly labeled volume mounted on a storage device, the NetWorker server requests that such a volume be mounted and waits until an operator or an autochanger mounts an appropriate volume.

### Default media pool

If the save stream does not match the criteria for any custom (user-created) media pools, the NetWorker server directs the save stream to the Default media pool. Even if you use customized media pools, ensure that appropriate storage devices and media are available for the Default media pool for cases when the NetWorker server directs save streams there. If the media pools are not properly configured for backup, an error message similar to this may appear in the Monitoring Alerts tab in the Administration window:

```
media waiting (or critical): backup to pool 'Default' waiting for 1
writable backup tape or disk
```

## NetWorker media pool types

NetWorker software contains preconfigured media pool types to keep different types of data separate. NetWorker software does not mix these types of data within a media pool:

- Backup
- Backup clone
- Archive
- Archive clone
- Migration

- Migration clone
- WORM (Write Once-Read Many)
- DLTWORM

Without any special sorting, all backup data is routed to the Default media pool and all archive data is routed to the Default Archive media pool. Likewise, clone data is routed to the appropriate Default Clone media pool.

## Sorting data with media pools

When you configure the NetWorker server, you can create additional media pools and sort data by media pool type and any combination of the following:

- Group (backup group)
- NetWorker client
- Save sets (file or file systems)
- Backup levels (full, levels 1 – 9, incremental, manual)

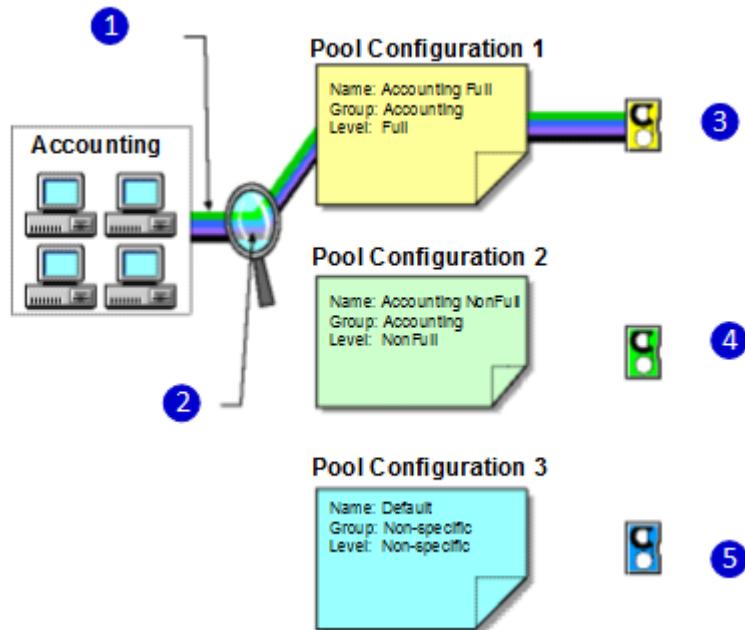
When you select a group, the media pool accepts only data associated with the named group. If a second group name is added, the media pool accepts data associated with either group, but no others. If you enter configuration criteria in both the Group attribute and Save Set attribute, only data that meets both the group criteria and the save set criteria is written to volumes from the specified media pool.

## How media pool configurations sort data example

This figure illustrates how the NetWorker server uses media pool configurations to sort data. The save stream contains data from a full backup that was performed on client and save sets in a group called Accounting. The NetWorker server looks for a media pool configuration that matches the group named Accounting and the level full. When the NetWorker server finds the matching media pool configuration, it writes the data to a volume with a label from the corresponding Accounting Full media pool of volumes mounted on one of the storage devices.

In this figure, the numbers represent the following:

1. The save stream from the full backup of the Accounting group
2. NetWorker looks for a matching pool configuration
3. Volume from the Accounting Full pool. The label is AccountingFull.001
4. Volume from the Accounting Non-Full pool. The label is AccountingNonFull.001
5. Volume from the Default pool. The label is Default .001

**Figure 25** Using media pool configurations to sort data

## Directing client file indexes and bootstrap to a separate media pool

You can use regular expression matching to direct the client file indexes and bootstrap to a media pool other than where you send the backup data.

### Sending bootstrap information and all the client file indexes to the same media pool example

To send the NetWorker server's bootstrap and client file indexes to the same media pool, create a media pool (in the Media Pool resource) with the values listed for the attributes in this table.

**Table 42** Attributes to direct client indexes and bootstrap to a separate media pool

Attribute	Value
Name	Index
Pool Type	Backup
Save Sets	Bootstrap index

When the group's scheduled backup runs, the client save sets are written to a volume labeled for the appropriate save set media pools, while the NetWorker server's bootstrap and index save sets are written to a separate volume labeled for the Index media pool.

## Directing consolidated backup data to a specific media pool

By default, save sets from a consolidated backup are written to whatever media is mounted for the group most recently backed up.

### Procedure

1. Configure a **Group** resource for consolidated backups.

2. Configure a **Media Pool** resource for consolidated backups.
3. In the **Create Media Pool** dialog box, select the name of the **Group** resource created in step 1 for the **Groups** attribute.
4. Add each client that will receive consolidated backups to the group created for those backups.

## Meeting the criteria for more than one media pool configuration

Depending on the media pool that is created, there may be data that matches the criteria for more than one media pool configuration. For example, if one media pool is configured to accept data from a group called Accounting and another media pool is configured to accept data from all full backups, it is not immediately clear which pool of volumes will be used for a full backup for the Accounting group. The NetWorker server uses this media pool selection criteria:

1. Group (highest precedence)
2. Client
3. Save set
4. Level (lowest precedence)

When data matches the attributes for two media pools, for example, Group and Level, the data is written to the media pool specified in the Group attribute. For example, in the case where the data from the group matched the criteria for two different media pools, the data is routed to the media pool that accepts data from the Accounting group.

The following table details the hierarchy that the NetWorker server uses to determine media pool selection when a conflict arises. For example, the media pool criteria for Group takes precedence over the media pool criteria for client, save set, and level. Data that meets the criteria for both media pools is written to the media pool associated with the group. If data does not meet the criteria for any customized group, it is written to the Default media pool.

**Table 43** NetWorker hierarchy for resolving media pool conflicts

Precedence	Group	Client	Save Set	Level
Highest	x	x	x	x
	x	x	x	
	x	x		x
	x	x		
	x		x	x
	x		x	
	x			x
		x	x	x
		x	x	
		x		x

**Table 43** NetWorker hierarchy for resolving media pool conflicts (continued)

Precedence	Group	Client	Save Set	Level
			x	
Lowest				x

## When no customized media pool criteria is met

When you sort data by using a customized media pool, you might inadvertently omit a client or save set. During a scheduled backup, if data does not meet the criteria for any customized media pool, the NetWorker server automatically sends the data to the Default media pool. By using the Default media pool, the server ensures that all data is backed up to a volume.

When the NetWorker server sends data to the Default media pool, it looks for a labeled volume from the Default media pool mounted on a storage device. If no Default media pool volume is mounted on a storage device, the server requests the appropriate volume and waits until an operator mounts the volume. If the NetWorker server asks for a Default media pool volume in the middle of a scheduled backup, the backup pauses until it has been mounted. If an operator is available to monitor backups, keep a Default media pool volume on hand should this situation arise.

To plan for unattended backups, run a test of the backup after making any configuration changes. This ensures that all data is written to the appropriate media pools of volumes, and avoids requests for a Default media pool volume.

## Media pool configurations

This section provides information specific to the configuration of these media pool types:

- Incremental backups
- Manual backups
- Clone data
- Archive data

### Note

You can create and edit media pools while a backup session is running. For each change, a message is written to the daemon log file, located in the `<NetWorker_install_dir>\logs` directory. You cannot delete a media pool that has labeled volumes in the media database.

## Incremental backups

When creating a separate media pool for incremental backups, the NetWorker software's hierarchy of precedence affects the way the data is stored. When a pool has been configured with a level incremental restriction and an incremental server initiated backup is performed:

- Incremental data will be routed to the media pool.
- The client file index will not go to the incremental pool. In an incremental backup, the associated index will backup at a level 9 to speed the recovery operation, if needed.

If the client indexes do not meet the criteria for the media pool associated with the incremental backups (that is, level 9 is not allowed), the indexes are matched to another

media pool (usually the Default media pool) and an appropriately labeled volume is searched for. To recover the data, a large number of volumes may be required. To speed the recovery, define the level value of the appropriate pool to accept both level 9 and incremental data, rather than only incremental.

By using the preconfigured NonFull media pool, you ensure that the client file indexes belong to the same media pool as their incremental backups. By keeping the indexes in the same media pool as their incremental backups, you reduce the number of volumes required for a recovery.

## Manual backups

You can create a customized media pool to receive data from a manual backup by specifying manual in the Level attribute. The NetWorker server, however, sorts data from a manual backup differently than it sorts data from a regularly scheduled backup. Since a manual backup is not performed as part of a scheduled backup group, by default the data is not associated with any group name. When you perform a manual backup in which only data from a single client or save set is saved, the group normally associated with that client or save set is not considered in any sorting. As a consequence, data from a manual backup may be sent to a media pool other than the one in which data from this client or save set is stored during a regularly scheduled backup. If you do not create a customized media pool to receive data from manual backups, the NetWorker server uses the Default media pool and looks for a mounted volume from the Default media pool on which to write data.

---

### Note

Manual backups only back up file system data. Unlike scheduled backups, they do not back up the client file index at the end of the backup. The next server initiated backup of the client will backup the index. Manual backups can still be browsed at recovery time unless an index recover is performed before the index containing the save information has been backed up.

---

## Clone data

To clone data, use a specific media pool to receive the clone data and a minimum of two devices:

- One to read the source volume
- One to write the clone

If data to be cloned is not associated with a customized Clone media pool, the Default Clone media pool is used.

## Archive data

To archive data, use a specific media pool to receive the archived data. You can then store these volumes offsite. If data to be archived is not associated with a customized Archive media pool, the preconfigured Archive media pool is used.

## Using storage devices and media pool configuration to sort data

Data can be sorted by configuring media pools, in conjunction with storage devices, to either use specific media to receive data, or designate a specific storage device to receive data from a designated media pool.

## Using different media

You can write data across several volumes of different media types (for example, magnetic disk and tapes) as long as the volumes mounted on the storage devices have the appropriate label associated with the media pool.

## Using a specific device for backup data

You can associate a media pool with a specific storage device. For example, full backups may be written to optical disk for offsite storage. There are two ways to ensure that data goes to one specific storage device:

- Always keep a labeled volume associated with the appropriate media pool mounted on the specific storage device.
- Associate a specific media pool with the storage device in the Volume Pool attribute in the Device resource. Then, for the Media Pool resource, select that device for the Devices attribute. All data will be written only to that device.

---

### Note

The only time you can assign a device to a media pool is when you label it. If you later want to assign the device to a different volume pool, you must relabel it.

---

## Creating a media pool

Resource dialog box attributes vary depending on the server. Use the steps presented here as a general guideline. For additional information about each attribute, click Field Help.

Before creating a media pool, do either of the following:

- If the Match Bar Code Labels attribute is not used for the Library resource, create a label template for the media pool.
- Determine a preconfigured label template to use for the media pool.

If you do not select a label template when creating a media pool, the NetWorker server notifies you that it will create a label template for the media pool.

To have the NetWorker server create the label template, click OK.

### Procedure

1. In the **Administration** window, click **Media**.
2. In the left pane, select **Media Pools**.
3. From the **File** menu, select **New**.
4. In the **Name** attribute, type a name for the media pool.

A media pool is associated with a label template. Use a name that clearly associates the media pool with the corresponding label template.

5. In the **Comment** attribute, type a description of the media pool.
6. Select the **Enabled** attribute.
7. For the **Pool Type** attribute, select the appropriate media pool type.
8. In the **Label Template** attribute, select the matching label template.
9. In the **Data Source** attribute, select the backup groups that are eligible to back up to this media pool.

10. Select the **Selection Criteria** tab.
11. To further restrict which data can back up to this media pool, complete any of these attributes: **Client**, **Save Sets**, or **Level**.
12. Select the **Configuration** tab.
13. In the **Auto Media Verify** attribute, select whether automated media verification will be performed while data is written to a volume associated with this media pool.
14. Complete the other attributes as necessary, and click **OK**.

If any of the settings for a new media pool match an existing media pool, this message appears:

```
Pool(s) pool_name has overlapping selection criteria.
```

If this message appears, review the media pool configuration and modify any overlapping criteria.

## Expression matching of save sets to media pools

If you enter a save set path, the Save Set attributes in the Media Pool resource are matched by using regular expression matching. This affects how the save set filenames are written, and how the path is written in this field for a Microsoft Windows system. Backslashes and periods must be preceded with a backslash:

- A save set path of C:\SomeDir\MyFiles should be written C:\\SomeDir\\MyFiles.
- A filename of MyFile.txt should be written MyFile\\.txt.

When using the NetWorker Administrator program, each save set in the Save Set attribute must be on a separate line. The following is an example of properly written save set entries:

```
/  
/usr  
C:\\Program Files\\bin  
*\\.doc
```

The nsr\_regexp and nsr\_pool entries in the *EMC NetWorker Command Reference Guide* or the UNIX man pages provide information about regular expression matching.

## Auto media verification

If the Auto Media Verify attribute is enabled, the NetWorker server verifies data written to tape volumes from this media pool. This attribute does not apply to AFTD, file type and Data Domain devices.

Data is verified by repositioning the tape volume to read a portion of the data previously written to the media. The data read is compared to the original data written. This feature does not verify the entire length of the tape.

If the data read matches the data written, verification succeeds.

Media is verified when the following occurs:

- A volume becomes full while saving and it becomes necessary to continue on to another volume.
- A volume goes idle because all save sets being written to the volume are complete.

When a volume fails verification, it is marked full so that the server will not select that volume for future saves. The volume remains full until it is recycled or a user marks it not

full. If a volume fails verification while the server is attempting to switch volumes, all save sets writing to the volume are terminated.

Auto media verification should not be used to verify the integrity of the data written to the entire tape. To fully verify the data written to the tape, either restore the tape contents or clone the data.

## Managing volumes in a media pool

In NetWorker 8.0 and later, new pool resource attributes exist to provide support for scheduling the automatic relabeling of eligible volumes in a pool. In prior releases, volumes would be relabelled at the time of backup or clone and only when the selection criteria was met.

Consider the following:

- Automatically relabeling a recyclable volume provides the following benefits:
  - Volumes can be relabeled outside of the backup window without the need for a scripted solution.
  - Appendable volumes are available at the time of a backup or clone, resulting in faster backup and clone completion times.
- Eligible volumes will not be relabeled if the volume is loaded in a device that is:
  - Disabled
  - In use by an nsrmmdd process (for example, during a restore operation)
  - In read-only mode
  - Busy
- The daemon.raw file on the NetWorker server is updated with the following message when volumes are automatically relabeled:

```
"num_of_volumes volumes will be recycled for pool pool_name in
jukebox jukebox_name."
```

To configure automatic volume relabeling for a pool:

### Procedure

1. Modify an existing pool or create a new pool resource.
2. Under the **Miscellaneous** tab, configure the automatic relabeling attributes as required:
  - Recycle start: (Format HH:MM) defines the time to start the automatic relabel process each day. By default this attribute is empty and the automatic relabelling of recyclable volumes is not done.
  - Recycle interval: (Format HH:MM) defines the interval between two starts of automatic relabel processes. The default value is 24:00.
  - Recycle start now: invokes the automatic relabel process of recyclable volumes for this pool immediately. The default value is No.
  - Max volumes to recycle: defines the maximum number of recyclable volumes that can be relabeled during each automatic relabel process. The default value is 200.

## Supported WORM and DLTWORM tape drives

NetWorker supports write-once, read-many (WORM) tape drives and media. It is able to recognize the WORM abilities of tape drives and the presence of WORM media in those

drives. It also supports the creation of DLTWORM (formerly DLTice) tapes in drives that are DLTWORM capable.

The following table describes the WORM devices that are supported by the NetWorker software. For a complete listing of supported devices, refer to the *EMC NetWorker Hardware Compatibility Guide* on the EMC Online Support web site.

**Table 44** WORM supported devices

Device	Description
HP LTO Ultrium 3 and higher	Unique to HP Ultrium-3 and higher: <ul style="list-style-type: none"><li>• Inquiry VPD page 0xb0, byte 4 bit 0 indicates WORM capable</li><li>• Read attribute # 0x0408 bit 7 to indicate WORM media present</li></ul>
Quantum SDLT600, DLT-S4, and DLT-V4 (SCSI and SATA)	Any drive with product inquiry data of “*DLT*” tape drive that reports WORM capability the way these drives do (“Quantum” not required in the vendor inquiry data): <ul style="list-style-type: none"><li>• Inquiry data VPD page 0xc0, byte 2, bit 0 to indicate WORM capable</li><li>• Read attribute # 0x0408 bit 7 to indicate WORM media present</li></ul>
Sony AIT-2, AIT-3, AIT-4, and SAIT	Any drive with “Sony” in the vendor inquiry data that reports WORM capability like these drives do: <ul style="list-style-type: none"><li>• Mode sense page 0x31, byte 5 bit 0 indicates WORM capable</li><li>• Mode sense byte 4 bit 6 indicates WORM tape present</li></ul>
IBM 3592	Unique to IBM 03592: <ul style="list-style-type: none"><li>• Mode sense page 0x24, byte 7 bit 4 indicates WORM capable</li><li>• Mode sense page 0x23, byte 20 bit 4 indicates WORM tape present</li></ul>
STK 9840A/B/C, 9940B, T10000	Any drive with STK as the vendor data that reports WORM capability like these: <ul style="list-style-type: none"><li>• Standard inquiry data byte 55 bit 2 indicates WORM capable</li><li>• Request sense data byte 24 bit 1 indicates WORM tape present</li></ul>
IBM LTO Ultrium 3 and higher, and Quantum LTO Ultrium 3 and higher	These drives use the SCSI-3 method to report WORM capabilities, so there is not a match against any of the inquiry data. Any drive that does not match the inquiry data patterns listed above will have the SCSI-3 method applied to them: <ul style="list-style-type: none"><li>• Inquiry data VPD page 0xb0, byte 4, bit 0 indicates WORM capable</li><li>• Mode sense page 0x1d, byte 2 bit 0 indicates WORM tape present<ul style="list-style-type: none"><li>Byte 4, bits 0,1: label restrictions include<ul style="list-style-type: none"><li>- 00 indicates no overwriting allowed</li><li>- 01 indicates some labels can be overwritten</li></ul></li></ul></li><li>• Byte 5, bits 0,1: filemark overwrite restrictions<ul style="list-style-type: none"><li>- 0x02: any filemark at EOD can be overwritten except for the one closest to the beginning of the tape</li><li>- 0x03: any filemark at EOD can be overwritten</li></ul></li></ul>

The WORM and DLTWORM attributes determine whether or not the NetWorker software will back up to a write once-read many (WORM) tape. You can apply these tape attributes to any pool.

**Note**

Various Quantum drive models (SDLT600, DLT-S4, and DLT-V4) have the ability to create WORM tapes from ordinary blank DLT tapes supported by that particular drive. You cannot recycle an existing NetWorker tape to create a DLTWORM volume without first having bulk-erased the tape. When the DLTWORM attribute is set, labeling one of these drives into a WORM pool causes the Quantum drive to make the current tape a WORM tape.

Savegroups that belong to pools that have either the WORM or DLTWORM attribute set, are considered to be WORM savegroups.

## How to identify WORM media

Since WORM media cannot be reused, the tapes are uniquely identified as such so that they are only used when required. As shown in this figure, a (W) is appended to the volume names displayed in the NetWorker Administrator window. If a volume is both read-only and WORM, an (R) is appended to the volume name.

**Figure 26** Identifying WORM tapes in the NetWorker Console

Volume Name	Barcode	Used	% Used	Mode	Expiration	Location	Pool
000000	000000	0 KB	0% appen				Default
000016	000016	0 KB	0% appen				Default
000017	000017	0 KB	0% appen				Default
000018	000018	0 KB	0% appen				Default
000024	000024	0 KB	0% appen				Default
000134(W)	000134	0 KB	0% appen	manual	rd=aurora:A...	WORM	
alt2_worm.001(W)		0 KB	0% appen	manual		worm	
ameba.003		0 KB	0% appen			Default	
arch_talks_backup_12_05_2005		194 GB	97% appen	manual		Default	
berferd.001		152 GB	95% appen	manual		worm	
bobs_first_tape(R)		34 GB	17% recyc	expired		Default	
dtv4_worm_001		0 KB	0% appen		9	Default	
dtwrm.001		0 KB	0% appen	manual		worm	
fatdat.ameba.001(R)		1356 MB	2% recyc	expired	9	Default	
NEGVAR.DDS.001(R)		269 MB	0.1% recyc	expired		Default	
not_the_worm.001		15 GB	15% appen			Default	
not_worm_new.001		0 KB	0% appen		9	Default	
salt_via_polarbear.001		1091 MB	full	9/12/06		Default	

**Note**

Since WORM tapes can only be used once, attempting to relabel a WORM tape always results in a write protection error. With the exception of pool selection and relabeling, the NetWorker software treats WORM tapes exactly the same as all other types of tape.

## Determining WORM and DLTWORM capability

**Note**

The WORM capable and DLTWORM capable attributes are dimmed out when the device in use is WORM capable but does not support DLTWORM (not a Quantum DTL-type drive).

**Procedure**

1. In the Administration window, click Devices.
2. Select the drive, right-click, and select Properties.

3. Click the **Information** tab and observe the WORM capable and DLTWORM capable attribute settings. NetWorker automatically sets these attributes and, consequently, they are read-only and cannot be changed.

## Configuring WORM and DLTWORM support

The following table describes WORM and DLTWORM attributes.

**Table 45** WORM/DLTWORM attributes

Attribute	Description
WORM pools only hold WORM tape	By default, the NetWorker software only allows WORM tapes into WORM pools. Deselecting this option lets you add new (non-WORM) tapes to a WORM pool. This is useful when you need WORM functionality but do not have WORM tapes available.
WORM tapes only in WORM pools	By default, NetWorker only lets you label WORM tapes into WORM pools. Clear this option when: You do not want to segregate WORM tapes within WORM pools. A volume is needed to complete a group and a non-WORM tape is unavailable.
WORM capable	This attribute indicates that this drive supports the use of WORM media.
DLTWORM capable	This attribute indicates that this drive can create DLTWORM tapes from a blank tape.
WORM pool	This pool should hold WORM tapes (depending on the setting of “WORM pools only hold WORM tape” in the server).
create DLTWORM	If selected, before the NetWorker software labels a tape in a drive capable of creating DLTWORM volumes, NetWorker will try to convert the tape into a DLTWORM tape. If that conversion fails, the labeling for that tape will fail. If a tape drive in a pool where this attribute is set cannot create DLTWORM tapes, (that is, the tape drive is not a Quantum SDLT600, DLT-S4 or DLT-V4 tape drive, this attribute is simply ignored). Refer to the Quantum web site for information on which tapes can be converted to DLTWORM tapes.  Not all firmware revisions for all of these devices support WORM operation. Check the tape drives website to make sure that your drive has up-to-date firmware.

## Procedure

1. In the **Administration** window, click **Media**.
2. In the left pane, select **Media Pools**.
3. In the right pane, select the appropriate pool.
4. Right-click and select **Properties**.
5. Click the **Configuration** tab and select one of these WORM tape handling attributes:
  - WORM pools only hold WORM tapes
  - WORM tapes only in WORM pools
6. Click **OK** when finished making the necessary selections.

---

**Note**

If you attempt to assign a non-WORM capable drive to a WORM pool an error message is generated.

---

## Working with media pools

This section explains how to edit, copy, delete, and create media pools.

### Editing a media pool

---

**Note**

You cannot change the name of a media pool. Preconfigured media pools cannot be modified.

---

**Procedure**

1. In the **Administration** window, click **Media**.
2. In the left pane, select **Media Pools**.
3. In the right pane, select the media pool.
4. From the **File** menu, select **Properties**.
5. In the **Properties** dialog box, make the necessary changes and click **OK**.

### Copying a media pool

For details about the Media Pool attributes, click Field Help in the Properties dialog box.

**Procedure**

1. In the **Administration** window, click **Media**.
2. In the left pane, select **Media Pools**.
3. In the right pane, select the media pool.
4. From the **Edit** menu, select **Copy**. The **Create Media Pool** dialog box appears, containing the same information as the media pool that was copied, except for the **Name** attribute.
5. In the **Name** attribute, type a name for the new media pool.
6. Edit any other attributes as appropriate, and click **OK**.

### Deleting a media pool

---

**Note**

You can delete a media pool only if there are no active volumes assigned to the media pool. Preconfigured media pools cannot be deleted.

---

**Procedure**

1. In the **Administration** window, click **Media**.
2. In the left pane, select **Media Pools**.
3. In the right pane, select the media pool.
4. From the **File** menu, select **Delete**.
5. When prompted, click **Yes** to confirm deletion.

## Creating an archive media pool

To archive data, the NetWorker server requires an archive media pool to receive the archive data. If data to be archived is not associated with a custom archive media pool, the server automatically uses a preconfigured archive media pool. An appropriately labeled volume must be mounted on a storage device for the archive process to proceed.

### Procedure

1. Create a new media pool.
2. From the **Pool Type** attribute, select **Archive** from the list.
3. Select the **Configuration** tab.
4. Clear the **Store index entries** attribute.

## Label templates

The NetWorker server creates a unique label for each volume by applying a label template. This section describes how label templates and media pools are used to sort, store, and track data on media volumes.

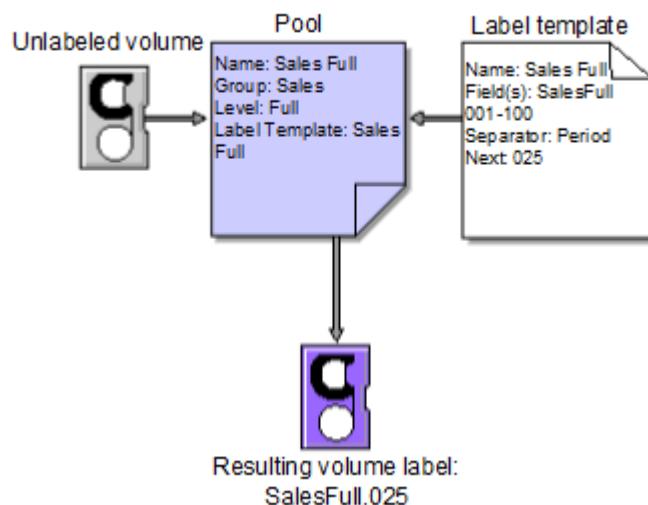
## Using label templates

The NetWorker server selects the media pool to which a given set of data is written. A volume is associated with a media pool by its volume label.

The contents of the volume label follow rules that are defined in a specific label template. You then associate a label template with a specific media pool in the Media Pool resource. If you do not associate data with a specific media pool, the NetWorker server uses the preconfigured Default media pool and corresponding Default label template.

The following figure illustrates how a media pool configuration uses its associated label template to label a volume. For the label template name to appear as a choice in the Media Pool resource, you must configure a label template before configuring the associated media pool.

**Figure 27** Labeling a volume by using a label template



## Preconfigured label templates

The NetWorker server contains these preconfigured label templates, which correspond to the preconfigured media pools:

- Default
- Default clone
- Archive
- Archive clone
- Full
- Indexed archive
- Indexed archive clone
- NonFull
- Offsite
- PC archive
- PC archive clone
- Two Sided

Label templates have multiple fields separated by periods. The first field represents the name of the NetWorker server and the final field contains a number to allow for expansion of the media pool. The number range from 001 to 999. For example:

```
mars.001
jupiter.054
jupiter.archive.197
```

## Guidelines for completing Label Template attributes

There are certain guidelines to keep in mind when completing the attributes for a Label Template resource. The following table describes how to complete the key attributes for this resource.

**Table 46** Key label template attributes

Attribute	Guidelines
Name	Keep the label name consistent with the media pool name, so that the label name reflects how the data is organized. For example, a label template named "AcctFull" would identify volumes that belong to a media pool called "Accounting Full." Do not use these characters in label template names: / \ * ? [ ] ( ) \$ ! ^ ; , " ' ~ < > &   { } : - . _
Fields	A label template is made up of one or more fields. Each field, or component, provides a layer of specificity to your organizational structure. There can be any number of components, but it is best to keep the template simple with as few as necessary. The label cannot exceed 64 characters. You can use four types of components: <ul style="list-style-type: none"> <li>• Range of numbers (for example, 001-999)</li> <li>• Range of lowercase letters (for example, aa-zz)</li> <li>• Range of uppercase letters (for example, AA-ZZ)</li> </ul>

**Table 46** Key label template attributes (continued)

Attribute	Guidelines
	<ul style="list-style-type: none"> <li>Character string (for example, Accounting) Each range includes a start value, a dash (-), and an end value. The start value and the end value must have the same number of characters. For example, use 01-99 (not 1-99) or aaa-zzz (not aa-zzz).</li> </ul> <p>The order in which you enter each component of the Field attribute is important. The NetWorker server applies each component in a left-to-right order, starting with the first one entered.</p>
Separator	Choose the symbol to appear between component entries. Use the period, dash, colon, or underscore to separate each component of the label template. If label components do not have separators (for example, AA00aa), the labels can be difficult to read.
Next	<p>Choose the next sequence number to write on the label that the NetWorker server places on a volume (according to the template).</p> <ul style="list-style-type: none"> <li>To force a label to start the label scheme at a particular point, type a start label value. The server continues to generate labels from that point on, according to the rules of the template.</li> <li>To have the NetWorker server generate the first label, leave this attribute blank. When the NetWorker server recycles a storage volume, the volume label does not change as long as the volume remains in the same media pool. That is, if a storage volume labeled "Dev.006" is recycled, it retains the volume label "Dev. 006" and does not receive a new label with the next sequence number.</li> </ul>

The following table lists examples of number sequences for volume labels.

**Table 47** Examples of number sequences for volume labels

Type of components	Fields	Number sequence result	Total number of labels
Range of numbers	001-100	001, 002, 003,...100	100
Character string Range of numbers	SalesFull 001-100	SalesFull.001,...SalesFull.100	100
Range of lowercase letters Range of numbers	aa-zz 00-99	aa.00,...aa.99, ab.00,...ab.99, ac.00,...ac.99, : az.00...az.99, ba.00,...ba.99 : zz.00,...zz.99	67,600 (262 times 102)

The label template should allow for expansion of the backup media storage system. For example, it is better to create a template for 100 tapes and not use all of them, than it is to create a template for only 10 tapes and run out of labels. When the server reaches the end of the template numbering sequence, it wraps to the starting value. For example,

after zz.99 (used for the 67,600th label), the next label the server uses is aa.00 for label 67,601.

#### Note

When the NetWorker server recycles a volume, the volume label does not change if the volume remains in the same media pool. That is, if a volume labeled Dev.006 is recycled, it will retain the volume label Dev.006 and will not receive a new label with the next sequence number. The original data on the volume, however, will be overwritten by the new data.

## Naming label templates

The NetWorker server is packaged with preconfigured label templates that correspond to the preconfigured media pools. If you choose to create the templates, you can include any number of components in the Fields attribute. However, it is best to keep the template simple with as few components as necessary for your organization.

For example, if you create a label template for an accounting department, you can customize the label template in several ways, depending on the size of the storage system and media device capabilities.

The following table illustrates several ways you can use components to organize labels.

**Table 48** Using label template components

Type of organizational structure	Components	Separator	Resulting volume labels
Sequential	AcctFull '001-100	period	AcctFull.001 (100 total labels)
Storage oriented (for example, 3 storage racks with 5 shelves each, each shelf holding 100 tapes)	1-3 1-5 001-100	dash	1-1-001 This label is for the first tape in rack 1 on shelf 1. (1,500 total labels)
Two-sided media (for example, optical devices)	AcctFull 000-999 a-b	underscore	AcctFull_000_a (side 1) AcctFull_000_b (side 2) (2,000 total labels)

## Tips for labelling

Naming schemes vary from site to site. One way is to name the volumes with the name of the NetWorker server followed by a three-digit number, for example:

```
jupiter.001
```

Consider that the simpler a convention is, the easier it can be understood by operators and administrators.

The maximum length for a volume name is 63 characters. With advanced file type devices (adv\_file), the maximum length is 60 characters.

Each volume should have a physical (adhesive) label attached to it. Since the NetWorker server keeps track of the backups and which volumes they are on, you can name the volumes with any convenient name. For example, you can label your volumes 1, 2, 3, or

Monday.1, Tuesday.1, Wednesday.1. You can assign a volume any name as long as each one is unique.

The adhesive label on the volume should match the name generated by NetWorker. For example, if you physically label a volume mars.1, its NetWorker name should also be mars.1.

## Working with label templates

This section explains how to create, edit, copy, and delete label templates.

### Creating a label template

When creating a label template, consider the labeling guidelines for the Name, Fields, Separator, and Next components.

#### Procedure

1. In the **Administration** window, click **Media**.
2. In the expanded left pane, select **Label Templates**.
3. From the **File** menu, select **New**.
4. Enter the components for the label template:
  - **Name:** The name of the new label template.
  - **Comment:** Any user-defined description or explanatory remarks about the label.
  - **Fields:** A list of label components.
  - **Separator:** The character to be inserted between label components. If no symbol is selected, the components will have no separators, such as hostarchive[001-999].
  - **Next:** (Optional) Enter the next label to be generated by the template.
5. Click **OK**.

### Editing a label template

You cannot change the name of a label template. However, to change an individual label name, delete the existing name in the Next text box, and type a new name.

#### Procedure

1. In the **Administration** window, click **Media**.
2. In the expanded left pane, select **Label Templates**.
3. In the right pane, select the template to edit.
4. From the **File** menu, select **Properties**.
5. In the **Properties** dialog box, make any necessary changes and click **OK**.

### Copying a label template

#### Procedure

1. In the **Administration** window, click **Media**.
2. In the expanded left pane, select **Label Templates**.
3. In the right pane, select the label template to copy.
4. From the **Edit** menu, select **Copy**. The **Create Label Template** dialog box appears, containing the same information as the label template that was copied, except **Name** attribute.

5. In the **Name** attribute, type the name for the new label template.
6. Edit any other attributes as appropriate, and click **OK**.

## Deleting a label template

You cannot delete a preconfigured label template or a label template that is in use.

### Procedure

1. In the **Administration** window, click **Media**.
2. In the expanded left pane, select **Label Templates**.
3. In the right pane, select the label template to delete.
4. From the **File** menu, select **Delete**.
5. When prompted, click **Yes** to confirm the deletion.



# CHAPTER 11

## Archiving

This chapter contains the following topics:

- [Overview of archiving](#)..... 306
- [Permissions for archiving](#)..... 308
- [About archive pools](#)..... 309
- [Attributes of Archive pools](#)..... 309
- [Archiving data procedures](#)..... 309
- [Retrieving archived data](#)..... 313
- [Archive request management](#)..... 316

## Overview of archiving

The archive process captures files or directories as they exist at a specific time, and writes the data to archive storage volumes, which are not automatically recycled. After the archive process completes, you can delete ([groom on page 755](#)) the original files from the disk to conserve space.

Archive save sets are similar to backup save sets. The main difference is that archive save sets have no expiration date. By default, the archive backup level is always set to full. Archive data must be written to separate pools. Browse and retention policies do not apply to archive data.

---

### Note

The archive feature must be purchased and licensed separately from other NetWorker software components. The *EMC NetWorker Licensing Guide* provides more information on licensing procedures.

Benefits of using the NetWorker archive feature include:

- Files that have been archived can be:
  - Deleted from the primary disk storage to make space for newer files.
  - Retained in archive volumes for quick retrieval.
- Archived data is never subject to automatic recycling, so it cannot be overwritten accidentally.
- Files on archived volumes that use the Indexed Archive pool and the PC Archive pool can be browsed indefinitely.

The NetWorker software does not support archiving of the WINDOWS ROLES AND FEATURES save set. The NetWorker Client Direct feature does not support archiving.

## Archive requirements

Before NetWorker archive feature, ensure that you have:

- A device, either stand-alone or in an autochanger or silo, connected to a NetWorker server or storage node. If you are cloning archives, you must have at least two devices available.
- A temporary or permanent enabler code to license the product after any evaluation period is over. The *EMC NetWorker Licensing Guide* provides more information.

## How the NetWorker server archives data

The NetWorker software provides three preconfigured pools to receive archived data:

- Indexed Archive pool
- PC Archive pool
- Archive pool

You can also create custom archive pools. During the archive operation, the NetWorker server writes data to storage volumes that belong to an Archive pool. Information about archive data is tracked in the NetWorker server's media database.

If you use the preconfigured Indexed Archive pool or PC Archive pool, or if you create a custom Archive pool that has the Store Index Entries attribute in the Pool resource set to Yes, information about individual files in the archive save set are tracked in the client file

index. The client file index entries that are generated during an archive are backed up to volumes from the Default pool during the next scheduled backup.

#### Note

Index entries are not generated when the Store Index Entries attribute in the Pool resource is set to No.

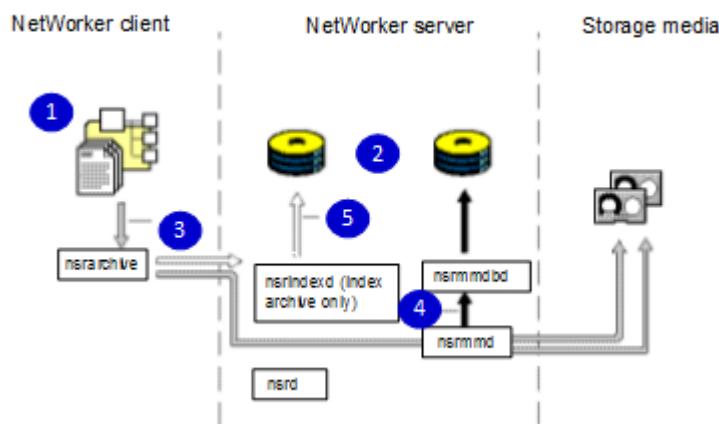
The NetWorker server tracks the volumes used for archives separately from those used for backups. You cannot archive files to a backup volume, nor can you back up files to an archive volume. An archive volume must be loaded and mounted in the server device to complete an archive.

Whether you initiate the archive on the client or the server, the archive is created by the client's archive program (nsarchive), which is initiated by the client's nsreexecd service. You can schedule archives from the server or client by using the Archive Requests resource in the NetWorker Administrator program.

The following figure illustrates how the NetWorker software archives data:

1. Client file systems
2. Backup data tracking structures
3. Data
4. Media database info
5. File index info

**Figure 28** Overview of archive operation



## Indexed and nonindexed archiving

The NetWorker server supports two styles of archiving:

- Indexed archiving for Indexed Archive pools or PC Archive pools
- Nonindexed archiving for Archive pools

### Indexed archiving (Indexed Archive pool, PC Archive pool)

One can browse and select indexed archives for individual file recovery.

To use indexed archiving, do one of the following:

- Use the preconfigured Indexed Archive pool or the PC Archive pool.

- Enable the Store Index Entries attribute of the Pool resource associated with the archive volume.

The client file index entries that are generated during an archive are backed up to volumes from the Default pool during the next scheduled backup.

## Nonindexed archiving (Archive pool)

When data is archived by using nonindexed archiving, entries are not added to the client file index. When this data is retrieved, the entire save set is retrieved and you cannot browse or recover individual files.

# Permissions for archiving

This section describes the permissions required to use the archive feature.

## Enabling archive services for the client

After the archive service is licensed and the enabler code has been entered into the NetWorker server, all clients of that server are enabled for the NetWorker archive feature by default. To disable the archive feature for a specific client, set the Archive Services attribute in the Client resource to Disabled.

To archive data that resides on the NetWorker server, ensure that the Archive Services attribute is enabled in the Client resource for the server.

When you enable the Archive Services attribute for a Client resource, enable the Archive Services attribute for all other clients of the same name on that server. For example, if the NetWorker Module for a database application and the NetWorker client software are installed on the same computer and both back up to the same NetWorker server, both Client resources have the same name. Ensure that the Archive Services attribute is enabled for both Client resources.

## Enabling or restricting archive access

The Archive Users User Group specifies the users who are allowed to archive data. The EMC NetWorker Security Configuration Guide provides more information.

Users can only retrieve data that they own. If other users need to retrieve data they do not own, then enable public archives access.

## Enabling public archive access

To allow users listed in the Archive User Group to retrieve any archived files from a client:

### Procedure

1. In the **Administration** window, click **Configuration**.
2. In the left pane of the **Configuration** window, select the NetWorker server.
3. From the **File** menu, select **Properties**.
4. Select the **Public Archives** attribute and then click **OK**.

### Results

If, during recovery, the operating system allows you to change the ownership of archived data to that of the original owners, then the retrieved files display the original ownerships. Otherwise, the user who retrieves the files becomes the owner of the files.

## About archive pools

The NetWorker software provides these three preconfigured pools to receive archived data:

- Preconfigured Indexed Archive pool
- PC Archive pool
- Preconfigured Archive pool

You cannot change the settings for these preconfigured pools, although you can create custom pools for archiving data. Custom pools can use either indexed or nonindexed archiving.

If you do not specify a pool to store archived data, the NetWorker software uses the Indexed Archive pool by default.

### Preconfigured Indexed Archive pool and PC Archive pool

The preconfigured Indexed Archive pool and the PC Archive pool store entries for individual files in the client file index.

---

#### Note

Use of the Indexed Archive pool or the PC Archive pool may create a large client file index that never expires.

---

### Preconfigured archive pool

The preconfigured Archive pool does not have a browsable client file index associated with it. You cannot retrieve individual files from the archive save set. Instead, you must retrieve the entire save set.

## Attributes of Archive pools

Two attributes in the Pool resource distinguish Archive pools from other pools:

- Pool Type - This attribute must be set to Archive, which tells the NetWorker server that volumes belonging to this pool are used for archiving.
- Store Index Entries - This attribute determines whether the archive is an indexed or nonindexed archive:
  - If this attribute is set to No, entries are not written to the client file index (nonindexed archiving).
  - If this attribute is set to Yes, entries are written to the client file index (indexed archiving).

## Archiving data procedures

You can request manual archives from the client, or you can schedule archives from the server.

## Enabling archive services for a NetWorker client

---

### Note

If the NetWorker client is set up for encryption with the aes ASM, archive data will also be encrypted.

---

### Procedure

1. In the **Administration** window, click **Configuration**.
2. In the left pane of the **Configuration** window, select **Clients**:
  - a. If you are creating a new client, select **New** from the **File** menu.
  - b. If you are editing an existing client, select the client and then select **Properties** from the **File** menu.
3. On the **Globals (2 of 2)** tab, enable the **Archive Services** attribute. When you enable archive services for one Client resource, archive services are enabled for all Client resources with the same hostname.
4. Make the remaining configuration choices as appropriate. The computer is now an enabled archive client. However, an archive will not occur until it is requested.

## Manually archiving data

You can manually archive data at any time. Manually archiving data is similar to performing a manual backup.

### Performing a manual archive from a NetWorker client on Windows

---

### Note

Manual archives that are performed from a Windows client do not enforce global or local file (nsr.dir) directives. However, local directives (networkr.cfg) that are created with the NetWorker User program are enforced. Scheduled archives, enforce all directives.

---

### Procedure

1. In the **NetWorker > User** program, click **Archive** to open the **Archive Options** dialog box.
2. Type a comment in the **Annotation** attribute. This annotation is used to uniquely identify each archive save set during retrieval.

### Note

Consider adopting a consistent naming convention so that one can easily identify archives based on the annotation name.

---

3. From the **Archive Pool** list, select the appropriate archive pool.

### Note

Only pools with their **Pool Type** attribute set to **Archive** are listed.

---

4. Select the appropriate settings for these criteria:
  - To write a copy of each archive save set to a volume from an archive clone pool, select **Clone**.

- If you enable cloning, type or select an archive clone pool for the **Archive Clone Pool** attribute.
  - To instruct the NetWorker server to check the integrity of the data on the storage volume, select **Verify**.
  - To instruct the NetWorker server to remove the archived files from the disk, select **Grooming**.
5. Click **OK**. The **Archive browse** window appears.
  6. From the **File** menu, select **Mark** to select each file or directory for archiving. When you select an item for archiving, a check mark appears next to that item.

#### **Note**

To clear an item currently marked for backup, select **Unmark** from the **File** menu.

7. From the **File** menu, select **Start Archive**.
8. Click **OK** and the **Archive** browse window appears. The NetWorker server appears in the **Archive Status** window, which monitors the progress of the archive. When the NetWorker server is finished archiving, a message similar to this appears in the **Archive Status** window:

```
Archive completion time: 2-21-09 5:18p
```

9. If **Groom** was selected, the **Remove Archived File** dialog box prompts for confirmation before NetWorker software deletes archived files from the local disk.

## Perform a manual archive from a NetWorker client on UNIX

To perform a manual archive from a UNIX client, use the `nsrarchive` command. Information about this command is available in the *EMC NetWorker Command Reference Guide* or the UNIX man pages.

## Scheduling data archives

Unlike scheduled backups, scheduled archives run only once. The advantage of a scheduled archive is that the archive can be run when network traffic and computer use is low.

### Scheduling an archive

Before you can schedule an archive request, enable the **Archive Services** attribute in the **Client** resource.

#### **Procedure**

1. In the **Administration** window, click **Configuration**.
2. In the left pane, select **Archive Requests**.
3. From the **File** menu, select **New**.
4. In the **Name** attribute, type a name for the archive request.
5. In the **Comment** attribute, type a description of the archive request.
6. In the **Client** attribute, type the archive client's hostname.
7. In the **Save Set** attribute, type the pathnames of the files and/or directories to be archived.

---

**Note**

If you archive all of the client's save sets, set the **Grooming** attribute (on the **Running** tab) to **None**. If this attribute is set to **Remove**, all of the archived save sets will be deleted from the client computer.

- 
8. Type a comment in the **Annotation** attribute. This annotation is used to uniquely identify each archive save set during retrieval.
- 

**Note**

Consider adopting a consistent naming convention so that one can easily identify archives based on the annotation name.

- 
9. In the **Directive** attribute, select a directive if special processing is to occur during the archive process.
  10. From the **Archive Pool** attribute, select the appropriate pool from the list:

- To store the entire save set, select the preconfigured **Archive** pool. This pool does *not* store the client file index.
- To store the client file index in addition to the entire save set, select the preconfigured **Indexed Archive** or the **PC Archive** pool.

11. Select the **Running** tab.

12. For the **Status** attribute, indicate a start time for the archive:

- To begin the archive immediately, select **Start Now**.
- To begin the archive at a specified time, select **Start Later** and indicate a time in 24-hour format in the **Start Time** attribute.

13. For the **Archive Completion** attribute, type a notification for the NetWorker server to use after completing the archive.

14. Select the appropriate response for these options:

- To instruct the NetWorker server to remove the archive files from the disk, select **Remove** from the **Grooming** list.
- To instruct the NetWorker server to check the integrity of the data on the storage volume, select the **Verify** attribute.
- To write a copy of each archive save set to a volume in an **Archive Clone** pool, select **Yes** for the **Clone** attribute and select an archive clone pool from the **Archive Clone Pool** list.

15. Click **OK**.

**Results**

To view information about the status of an archive request, open the Archive Request Details window.

## Copying an Archive Request resource

For details about the Archive Request attributes, click Field Help in the Properties dialog box.

**Procedure**

1. In the **Administration** window, click **Configuration**.
2. In the left pane, select **Archive Requests**.

3. In the right pane, select the archive request to copy.
4. From the **Edit** menu, select **Copy**. The **Create Archive Request** dialog box displays the same information as the archive request that was copied, except for the **Name** attribute.
5. Type the name for the new archive request in the **Name** attribute, edit any other attributes as appropriate, and click **OK**.

## Changing the archive time

You can also schedule an existing archive by using the Schedule Archive operation in the Activities Monitor.

### Procedure

1. In the **Administration** window, click **Configuration**.
2. In the left pane, select **Archive Requests**.
3. In the right pane, select an archive request.
4. From the **File** menu, select **Properties**.
5. Click the **Running** tab.
6. In the **Start Time** attribute, type a new time in this format:

`HH:MM [a,p]`

7. Click **OK**.

## Editing an archive request

### Procedure

1. In the **Administration** window, click **Configuration**.
2. In the left pane, select **Archive Requests**.
3. In the right pane, select an archive request.
4. From the **File** menu, select **Properties**.
5. Edit the attributes of the archive request and click **OK**.

## Deleting an archive request

---

### Note

You cannot delete an archive request that is currently in use.

### Procedure

1. In the **Administration** window, click **Configuration**.
2. In the left pane, select **Archive Requests**.
3. In the right pane, select an archive request.
4. From the **File** menu, select **Delete**.

## Retrieving archived data

This section describes how to retrieve archived data.

## Retrieval permissions

The following restrictions apply when retrieving or recovering archived data:

- You must have read permissions to the archived data.
- If the Server resource's Public Archives attribute is enabled, all users listed in the Archive Users User Group can retrieve data (as long as they have read permissions to the data).
- If the Server resource's Public Archives attribute is disabled, only the users in the Archive Users User Group that own the file can retrieve the data.

---

### Note

If, during retrieval, the operating system allows you to change the ownership of archived data to that of the original owners, then the retrieved files display the original ownership. Otherwise, the user who retrieves the files becomes the owner of the files.

---

## Retrieving archives from a client on UNIX

To retrieve archive data for a UNIX client, use the `nsrretrieve` program.

---

### Note

You cannot browse the archive data on a UNIX client.

---

To retrieve archived data:

### Procedure

1. Mount the archive volume in the appropriate storage device.
2. Start the `nsrretrieve` program. Type:

### Results

```
nsrretrieve -s NetWorker_servername -A annotation -S ssid/cloneid -i_recover_option path
```

- `-s NetWorker_servername`—The hostname of the NetWorker server.
- `-A annotation`—Specifies the annotation string for the archive save set. You must specify at least one annotation or ssid.
- `-S ssid/cloneid`—Specifies the archive save set to recover. To recover a cloned archive save set, specify the ssid and cloneid. You must specify at least one annotation or ssid.
- `-i_recover_option`—Specifies how the NetWorker server should handle a naming conflict between a recovered file and an existing file.  
For example:
  - `iN` does not recover the file when a conflict occurs.
  - `iY` overwrites the existing file when a conflict occurs.
  - `iR` renames the file when a conflict occurs. The recover process appends a `.R` to each recovered file name.
- `path`—Specifies the file or directory to recover. When you do not specify a path, NetWorker recovers all data in the archive save set.

The `nsrretrieve` man pages and the *EMC NetWorker Command Reference Guide* provides more information about additional options available with the `nsrretrieve` command.

### Using the nsrretrieve command

In this example, suppose that archive A is annotated with Accounting\_Fed and archive B is annotated with Accounting\_Local.

- If you type this command:

```
nsrretrieve -A Accounting
```

No match is found and no archive is retrieved.

- If you entered this command:

```
nsrretrieve -A ting_L
```

Archive B is located.

## Retrieving non-indexed archives from a client on Windows

Data that was archived with a non-indexed archive pool (such as the Archive pool) must be retrieved by the entire save set rather than by file selection.

### Procedure

1. Mount the archive volume in the appropriate storage device.
2. Start the **NetWorker > User** program.
3. From the **Operation** menu, select **Archive Retrieve** to open the **Source Client** window.
4. Select a client to retrieve the archived data from and click **OK**. The **Archive Retrieve** window opens.
5. For the **Annotation String** attribute, type all or part of the annotation assigned to the save set when it was archived.

---

#### Note

If no annotation is entered, all archived save sets for the client appear.

6. Click **OK**. The **Save Sets** dialog box opens.
7. From the **Save Sets** dialog box, perform either of these functions, if necessary:
  - To view a list of volumes required to retrieve the data from this archived save set, click **Required Volumes**.
  - To type a new path for the location of the recovered data and to indicate what the NetWorker server should do when it encounters duplicate files, click **Recover Options**.
8. Select the archived save set to retrieve and click **OK**. The **Retrieve Status** window opens.

---

#### Note

You can also recover archived save sets by using save set recovery.

## Recovering indexed archive data from a client on Windows

Data archived by using the Indexed Archive pool and the PC Archive pool maintain information in the client file index about the individual files in the save set.

The archived files are recovered the same way as nonarchived files. To recover indexed archived files, the archive must have been saved by using the Indexed Archive pool, PC

Archive pool, or be a custom archive pool with the Store Index Entries attribute in the Pool resource enabled.

#### Procedure

1. Start the **NetWorker > User** program.
2. Click **Recover** to open the **Source Client** dialog box.
3. Select the source client whose data is to be recovered, and click **OK**. The local client is the default selection.
4. Select the destination client for the recovered data, and click **OK**. The local client is the default selection.
5. Select the files to be recovered and click the **Mark** button.
6. Click **Start**.

## Archive request management

This section describes how to work with scheduled archive requests.

### Starting a scheduled archive at any time

You can start a scheduled archive immediately rather than wait for the scheduled start time.

#### Procedure

1. In the **Administration** window, click **Monitoring**.
2. Select the **Archive Requests** tab.
3. Right-click the archive request and select **Start**.

### Stopping a scheduled archive while in progress

#### Procedure

1. In the **Administration** window, click **Monitoring**.
2. Right-click the archive request and select **Stop**.

### Disabling a scheduled archive

#### Procedure

1. In the **Administration** window, click **Monitoring**.
2. Right-click the archive request and select **Disable Archive**.

### Viewing details of a scheduled archive

To open the Archive Request Details window:

#### Procedure

1. In the **Administration** window, click **Monitoring**.
2. Right-click the archive request and select **Show Details**.

#### Results

The Archive Request Details window provides information about the completion of an archive request:

- The Completion Time displays the time the archive finished. This is the difference between the completion and start times of the archive.
- The success of the archive request is either completed, failed, or partial.



# CHAPTER 12

## Cloning

This chapter contains the following topics:

- [Overview of cloning](#) ..... 320
- [Save set cloning](#) ..... 320
- [Specifying browse and retention policies for clone data](#) ..... 328
- [Volume cloning](#) ..... 329
- [Recovering cloned data](#) ..... 329
- [Cloning archived data](#) ..... 332
- [Directing clones to a special storage node](#) ..... 334
- [Using file type devices for clone operations](#) ..... 337
- [Backup-to-tape for Avamar deduplication clients](#) ..... 338
- [Cloning with Data Domain devices](#) ..... 338
- [Using the nsrclone command](#) ..... 338

## Overview of cloning

Cloning allows for secure offsite storage, transfer of data from one location to another and verification of backups. Cloning can be performed on volumes and on save sets.

Information about the volumes, status, and history of cloning operations can be viewed and monitored from the Administration window. Clone-related messages are also logged to the NetWorker message file and the savegrp log file, which are located in the <NetWorker\_install\_dir>\logs directory.

There are two main methods of cloning:

- **Save set cloning:**  
Save sets can be cloned based on a schedule or on-demand by manual selection.
- **Volume cloning:**  
Backup volumes can be cloned on demand by manual selection.

### Note

Cloning works differently for deduplication devices. The *EMC NetWorker Avamar Integration Guide* and the *EMC NetWorker Data Domain Depulication Devices Integration Guide* provides more information.

## Cloning requirements

The following requirements apply when performing cloning operations:

- A minimum of two storage devices must be enabled: one to read the existing data and one to write the cloned data:
  - If libraries with multiple devices are used, the NetWorker server mounts the volumes required for cloning automatically.
  - If stand-alone devices are used, mount the volumes manually. A message displays in the Alert tab of the Monitoring option that indicates which volumes to mount.
- The destination volume must be a different volume from the source volume, and must belong to a clone pool.
- You must be a member of the NetWorker Administrators group. The EMC NetWorker Security Configuration Guide provides information.
- Only one clone of a particular save set can reside on a single volume. Therefore, if three clones of the same save set are specified, each clone is written to a separate volume.

## Save set cloning

NetWorker provides the ability to schedule clone operations by using a Clone user interface in NMC.

## Considerations for scheduled clone jobs

Be aware of the following considerations when setting up scheduled clone jobs.

## Scheduling multiple clone jobs to start at the same time

Do not schedule more than 30 clone jobs to start at the same time. Scheduling 30 or more clone jobs to occur at the same time may result in some clone jobs timing out and not completing.

## Mixing save sets from different source devices

Clone operations that mix save sets from different source devices, such as Data Domain devices, AFTD devices, or NDMP devices, may be written to different target volumes. Although this behavior is by design, you may prefer to write all save sets in the clone operation to the same clone volume.

If the clone operation includes save sets from different devices, and you want all save sets to be written to the same volume, include only one volume in the clone target pool.

## Unmounted clone source volumes on remote storage nodes

If the clone source volume is on a remote storage node and is unmounted, attempting to start a regular volume clone operation will not complete successfully, even if the source volume is mounted after the clone operation attempts to start. The clone program `nsrclone` will hang with the following message:

```
Server <server_name> busy, wait 30 second and retry
```

This issue does not occur in the following situations:

- If the storage node is on the NetWorker server, that is, when the storage node is not remote.
- If performing a clone controlled replication (optimized clone) operation.

## Snapshot with scheduled cloning

To set up a scheduled clone for a snapshot backup, you must specify the backup group to which the snapshot rollover belongs. When setting up a scheduled clone job, specify the backup group in the Save Set Filters tab.

## Clone resources that are created with the nsradmin program

Clone resources (known as NSR clone resources) that are created with the `nsradmin` command line program cannot be edited as scheduled clone resources in the NetWorker Administration graphical user interface.

To avoid this issue, perform one of the following:

- Create scheduled clone resources in the Administration interface.
- If you must create a NSR clone resource with the `nsradmin` program, create a corresponding NSR task resource with the `nsradmin` program. Together, these resources will enable you to edit the clone item as a scheduled clone resource in the GUI. The corresponding NSR task resource must have its name and action attributes specified as follows:
  - **name:** “clone.nsrclone\_resource\_name”
  - **action:** > “> NSR clone:nsrclone\_resource\_name”
 For example, if the NSR clone resource was named TestClone1, the name and action attributes of the NSR task resource would be:
  - **name:** **clone.TestClone1**

- **action: NSR clone: TestClone1**

These entries are case-sensitive.

## Setting up a scheduled clone job

### Procedure

1. From the **Administration** window, click **Configuration**.
2. In the expanded left pane, select **Clones**.
3. From the **File** menu, select **New**.
4. In the **Name** attribute, type a unique name to identify the scheduled clone resource. Type additional information in the **Comment** attribute if necessary.
5. If you wish to override the saveset's original browse and retention policies, select new policies in the **Browse** and **Retention** policies attributes.
6. To specify the storage node that will write data during the clone operation, select a storage node from the **Storage node to WRITE save sets attribute**. If a selection is made in this attribute, it will override any storage node selection criteria.

This attribute is used primarily in conjunction with the Storage node to READ save sets attribute to balance access to storage media across different storage nodes.

7. To specify the storage node that will read data during the clone operation, select a storage node value from the **Storage node to READ save sets attribute**. This attribute is visible only when Diagnostic mode is selected. Additionally, the selected storage node must be included in at least one of the following:
  - The **Recover storage nodes** or **Storage nodes** attribute of the NetWorker server's client resource.
  - The storage node listed in the **Read Hostname** attribute for the library resource, if a library is being used.
  - A storage node on which any device in the library is configured, if a library is being used.

This attribute is used primarily in conjunction with the Storage node to WRITE save sets attribute to balance access to storage media across different storage nodes and is not intended for use with standalone devices such as AFTD's, file type devices, Data Domain devices, and so on.

8. To specify the clone media pool to write data to during a clone operation, select a clone type media pool from the **Write clone data to pool** attribute. If no selection is made, clones will be written to the default clone pool.

Pools are used to direct backups to specific media volumes. This attribute is particularly useful when you want to ensure that only certain media types are used to hold clone data. For example, to ensure that this clone job only replicates to a certain type of disk, such as a Data Domain type disk, select a clone pool that uses only Data Domain type disks. Likewise, to ensure that this clone job only replicates to tape (tape out), select a clone pool that uses only tape devices.

9. Select **Continue on save set error** to force NetWorker to skip invalid save sets and to continue the clone operation. If this option is not selected (default setting), an error message will be generated and the clone operation will not continue if an invalid save set or invalid volume identifier is encountered.
10. To restrict the number of clone instances that can be created for any save set that is included in this particular scheduled clone operation, type a value in the **Limit number of save set clones** attribute. A value of zero (0) means that an unlimited number of clones may be created for this scheduled clone operation.

Consider limiting the number of save set clones in cases where the clone operation has not completed and is being retried. For example, if you type a value of 1 in this attribute and then retry a partially completed clone operation, only the save sets that were not successfully cloned the first time will be eligible for cloning. In this way, unnecessary clone instances will not be created.

Regardless of the value in this attribute, NetWorker always limits the number of save set clone instances to one per volume. A clone pool can have multiple volumes. This attribute limits the number of save set clone instances that can be created for a clone pool in a particular scheduled clone operation.

11. Select **Enable** to allow the clone job to run at its scheduled time.
12. In the **Start Time** attribute, click the up and down arrows to select the time to start the clone job. Alternatively, type the time directly into the attribute fields.
13. From the **Schedule Period** attribute, select **Weekly by day or Monthly by day** depending on how you want to schedule the clone job and then select the day(s) of the week or month on which the scheduled clone is to occur.
14. To repeat the clone job within a day, specify an **Interval** time in hours. For example, if the start time is **6 AM**, and the interval is 6 hours, then the clone job will run at 6 AM, 12 PM, and 6 PM.

If the Limit the number of save set clones value is set, then the repeat clone job will fail after the limit is reached.

15. Select the **Save Set Filters** tab to specify the save sets to be included in this scheduled clone job.
16. Select **Clone save sets that match selections** to limit save sets by various filter criteria or select **Clone specific save sets** to explicitly identify the save sets to be cloned.

To clone save sets that match selection criteria:

- Specify selection criteria to limit the save sets that will be included in this scheduled job. You can select the following criteria:
  - Groups (save groups), required for snapshot rollover clones.
  - Clients (Client resources)
  - Pools (backup pools ), you must select an archive pool for archive data.
  - Filter save sets by level (backup level)
  - Filter save sets by name (save set name as specified in the Client resource)
  - Include save sets from the previous (save sets from the past number of days, weeks, months, or years)
 

To display a list of the save sets that will be cloned based on the specified filter criteria, select **Preview Save Set Selection**.

To clone specific save sets:

- Type the specific save set ID/ clone ID (ssid/clonid) identifiers in the **Clone specific save sets** list box. Type each ssid/cloneid value on a separate line.
- You can query save set IDs / clone IDs through the Administration > Media user interface or by using the `mminfo` command.

17. Select **OK** to save the scheduled clone job.

## Starting a scheduled clone job manually

You can start a scheduled clone job at any time without affecting the regularly scheduled start time.

### Procedure

1. From the **Administration** window, click **Configuration**.
2. In the expanded left pane, select **Clones**.
3. Right-click on a clone resource in the right-pane and select **Start**.

### Results

You can also start a scheduled clone from the NetWorker Monitoring feature.

## Monitoring scheduled clone jobs

You can view the status of scheduled clone jobs in the Monitoring window. You can view the scheduled clone's last start and end time and you can view the completion status of each save set that is included in the scheduled clone.

---

### Note

If you change the clone times for an existing scheduled clone job, the Monitoring window will show the time of the old scheduled clone time until the updated schedule is executed.

---

## Setting up automatic cloning from a backup group

You can also set up automatic clone operations for a backup group. The clone operation can be set to start immediately after each save set in the group is backed up (immediate cloning) or the clone operation can be set to start only after all save sets in the group are backed up.

Immediate cloning operations can complete sooner because they can run in parallel instead of sequentially. Performance gains with immediate cloning are most noticeable when there are many savesets in the backup queue or when there are many savesets of different sizes. Immediate cloning is only supported with clone-controlled replication (CCR) using DD boost devices.

---

### Note

All of the save sets that are associated with the group are backed up the first time the automatic clone operation is run regardless of whether the previous backup was full or incremental. Subsequent automatic clone operations for the same group will clone only those save sets that have changed since the previous backup.

---

### Procedure

1. From the **Administration** window, click **Configuration**.
2. In the expanded left pane, select **Groups**.
3. Select the group in the right-pane.
4. From the **File** menu, select **Properties**.
5. Select the **Setup** tab.
6. Select the **Clones** attribute.

7. Select a value from the **Clone mode** attribute.

- Select **Start on save set completion** to start a save set clone operation after the save set is backed up. If this option is selected, the NetWorker server parallelism attribute must be set to a value of 2 or higher. To access the server parallelism attribute, right-click the NetWorker server name in the left pane of the **Administration window**, select **Properties** and then select the **Setup** tab.

This option is supported only when performing clone-controlled replication with DD Boost devices. If this option is selected for non-DD Boost devices, it will fall back to the Start on Group Completion option.

- Select **Start on group completion** to start clone operations only after all savesets in the group are backed up.

8. Select a clone pool from the **Clone pool** attribute.

## Viewing the clone status of a save set

To determine whether a save set on a volume has been cloned, or is itself a clone, check the Query Save Set tab window.

## Cloning a save set manually

To manually clone a save set, first query the database, select the save set, and begin the cloning operation.

### Procedure

1. From the **Administration** window, click **Media**.
2. In the expanded left pane, select **Save Sets**.
3. In the right pane, select the **Query Save Set** tab. Use the **Query Save Set** tab to specify options to limit the range of save sets displayed. All query options are optional except for the date. A date range must be selected.

---

### Note

The text boxes in the **Query Save Set** tab are case-sensitive.

4. Type values in any of these attributes to limit the search:
  - Client Name
  - Save Set
  - Save Set ID
  - Volume
  - Pool
5. Use the **Copies** attribute to limit the search to only those save sets that have already been cloned:
  - a. Select a boolean value of greater than (>), equal to (=), or less than (<) from the list.
  - b. Type the number of clones to complete the search criteria for the **Copies** attribute.

For example, to search for only those save sets that have been cloned at least twice, select greater than (>) and then type 1 as the number of copies.
6. Use the **Save Time** attribute to limit the search to a period of time in which the save set was created.

By default, yesterday is used for the start date, and today is used for the end date. This means that save sets backed up between yesterday at 12:01 A.M. and the current time will be displayed.

For the From and To date fields, any of these formats are acceptable:

- Written out completely (for example, November 1, 2009)
- Numerically as mm/dd/yy (for example, 11/01/09)
- Date and time selection from the list.

A long date range may result in too many selected save sets. This can increase response time or even require that you close and reopen the browser connection to the NetWorker Console.

7. Use the **Status** attribute to limit the search to save sets that have a particular status. The following table lists the values that can be selected.

**Table 49** Save set status settings

Status	Description
All	Select all options listed under Select from in the Status area.
Select from	<p>Select one or more of the following options:</p> <ul style="list-style-type: none"> <li>• Browsable: Select if the save set still has an entry in the client file index.</li> <li>• Recyclable: Select if all save sets have passed both the browse and retention policy time periods; the volume may now be available for automatic relabeling and overwriting (provided all save sets on the volume are recyclable).</li> <li>• Recoverable: Select if the entry for the save set has been removed from the client file index, but is still available for recovery from the media (that is, the volume has not passed its retention policy).</li> <li>• In-progress: Select if the save set is currently in the process of being backed up. In-progress save sets cannot be cloned.</li> <li>• Aborted: Select if the save set was either aborted manually by the administrator during a backup, or because the computer crashed. Aborted save sets cannot be cloned.</li> <li>• Suspect: Select if a previous attempt to recover the save set failed.</li> </ul>

8. Use the **Maximum Level** attribute to limit the search to save sets of a particular backup level.

The level All is specified by default. All the levels up to and including the selected level are displayed. For example:

- If you select level 5, save sets backed up at levels full, 1, 2, 3, 4, and 5 are displayed.
- If you select level Full, only those save sets backed up at level full are displayed.
- If you select All, save sets for all levels are displayed.

9. Click the **Save Set List** tab.

The save sets that fit the criteria appear in the Save Sets list.

10. Select the save sets to clone from the **Save Set** list.

11. From the **Media** menu, select **Clone**.

- 12.From the **Target Clone Media Pool** list, select a clone pool.
- 13.Click **OK**, then click **Yes** on the confirmation screen.

## Manual cloning of a save set example

In this example, a user has requested that the NetWorker administrator manually clone several save sets that are not included in an automatic cloning schedule.

The user must send the data to another company located out of country. The administrator must clone the most recent full backup, and any incrementals since the last full backup, to make sure that the most current data is sent.

To clone the save set, the NetWorker administrator must have this information:

- NetWorker client name
- Name of the save set
- Date the data was backed up

### Procedure

1. From the **Administration** window, click **Media**.
2. In the expanded left pane, select **Save Sets**.
3. In the right pane, select the **Query Save Set** tab.
4. In the **Client Name** attribute, type the client name.
5. In the **Save Set** attribute, type the save set name.
6. For the **Start Date** and **End Date**, type the dates used for the search.

---

#### Note

In this case, the administrator does not need to change or select any status choices other than the defaults.

7. Click the **Save Set List** tab. All save sets that meet the selection criteria appear in the **Save Sets** list.
8. Select the save sets to clone.
9. From the **Save Set List**, determine the size of the data and the original volume that contains the data to be cloned.
10. Mount the original volume.
11. From the **Media** menu, select **Clone**.
12. From the **Target Clone Media Pool** list, select a clone pool.
13. Click **OK** and then click **Yes** on the confirmation screen.

## Additional manual clone operations

This section covers operations that can be performed on both volumes and save sets that have been manually cloned.

### Viewing manual clone history

A dialog box appears that shows manual clone history information.

#### Procedure

1. From the **Administration** window, click **Monitoring**.

2. From the **Monitoring** menu, select **Show Manual Clone History**.

### Stopping a manual clone operation

The manual clone operation is stopped.

#### Procedure

1. From the **Administration** window, click **Monitoring**.
2. From the **Monitoring** menu, select **Show Manual Clone History**.
3. Select the clone operation to be stopped.
4. Click **Stop Selected Operation**.

## Specifying browse and retention policies for clone data

The browse and retention policy for clone data can be specified independently of the original save set. In this way, clone data can be browsed and recovered after the policies of the original save set have expired.

To specify the browse or retention policy for clone data, perform one of the following:

- Specify a browse and retention policy in a scheduled clone job.
- Specify a retention policy in the Clone pool.
- Specify a retention policy from the command prompt.

### Specifying a browse and retention policy in a scheduled clone job

To specify a browse and retention policy in a scheduled clone job:

#### Procedure

1. From the **Administration** window, click **Configuration**.
2. In the expanded left pane, select **Clones**.
3. From the **File** menu, select **Properties**.
4. Select new policies in the **Browse** and **Retention** policies attributes. When the scheduled clone job is next run, the cloned save sets will be given the new browse and retention policies.

### Specify a browse and retention policy from the command prompt

To specify a retention policy from the command prompt, perform one of the following:

- Use the `nsrclone` command with the `-y` option when creating a clone save set.
- Specify a retention policy for an existing clone save set by using the `nsrmm -e` command.

To specify a browse policy from the command prompt:

- Use the `nsrclone` command with the `-w` option when creating a clone save set. However, be aware that this will also change the browse policy of the original save set instance if the original save set's browse time has not passed and is earlier than the new browse time for the clone.

## Specifying a retention policy for a Clone pool

You can only specify a retention policy for cloned data in a pool resource.

### Procedure

1. In the clone pool to which clone backups will be directed, select the **Configuration** tab.
2. From the **Retention** policy list, select a retention policy, then click **OK**.

---

### Note

Retention policies that are specified in a scheduled clone job or from the command prompt, override the retention policy specified in a clone pool.

---

## Volume cloning

Volume cloning is the process of reproducing complete save sets from a storage volume to a clone volume. You can clone save set data from backup or archive volumes.

## Creating a clone volume

### Procedure

1. From the **Administration** window, click **Media**.
2. In the expanded left pane, select **Volumes**.
3. In the right pane, select the volume to be cloned.
4. From the **Media** menu, select **Clone**.
5. From the **Target Clone Media Pool** list, select a clone pool.
6. Click **Ok**, then click **Yes** on the confirmation screen.

## Viewing clone volume details

You can view the details of a clone volume, such as the amount of space used, mode, expiration date, pool, and save sets.

### Procedure

1. From the **Administration** window, click **Media**.
2. In the expanded left pane, select **Volumes**.
3. In the right pane, details for each volume are displayed in the table.
4. To view save set information for a volume:
  - a. In the right pane, select a volume.
  - b. From the **Media** menu, select **Show Save Sets**.

## Recovering cloned data

The NMC Recovery Wizard, the save set recovery option in NetWorker User, and the recover command provides you with the ability choose which volume (original or clone) to use when recovering data.

NetWorker decides which volume to use when you:

- Perform a browsable recovery in NetWorker User.
- Perform a browsable recovery with the recover command and do not specify the clone pool.
- Perform a save set recovery with the recover command and do not specify the cloneid of the clone save set.
- Allow the NMC Recovery Wizard to select the required volumes for recovery.

NetWorker bases the volume selection on the following criteria:

#### Procedure

1. The highest priority is given to the volume (clone or original volume) that has a complete, non-suspect save set status. A complete save set that is suspect has a higher priority than an incomplete non-suspect save set.
2. If the volumes still have equal priority, then priority is given to the mounted volume.
3. If the volumes are mounted, then priority is based on the media type. The media types from highest to lowest priority are:
  - a. Advanced file type device
  - b. File type device
  - c. Other (such as tape or optical)
4. If the volumes are not mounted, then priority is based on the media location. The media locations from highest to lowest priority are:
  - a. Volumes in a library.
  - b. Volumes in an AlphaStor or SmartMedia controlled library.
  - c. Volumes that are not in a library but are onsite (**offsite** flag is not set).
  - d. Volumes that are offsite (**offsite** flag is set).

#### Results

Use the nsrmm command to specify that a volume is offsite. For example:

```
nsrmm -o offsite -V volume_id
```

The volumes required for recovery appear in the Required Volumes window of the NMC Recovery Wizard and the NetWorker User (Windows) programs.

You can also run the scanner program on a clone volume to rebuild entries in the client file index, the media database, or both. After you re-create the entries, normal recovery is available.

## Recovering a clone save set from the command prompt

When you use the recover command to perform a browsable or save set recover, you can recover from the cloned save set.

## Performing a save set recover from a cloned save set example

To perform a save set recover from a clone, use mminfo to determine the cloneid of the save set, then specify the cloneid in the recover command.

#### Procedure

1. Use **mminfo** to determine the cloneid of the save set you want to recover:

```
mminfo -av -r volume, savetime, client, ssid, cloneid, name
```

volume	date	client	ssid	clone id	name
backup.001	05/03/2013	bu_iddnwserver	3644194209	1362492833	C:\ddlib
clone.001	05/03/2013	bu_iddnwserver	3644194209	1362493448	C:\ddlib

- Specify the SSID and cloneid in the **recover** command.

For example:

```
recover -S 3644194209/1362493448
```

## Performing a browsable recover from a clone save set example

To perform a browsable recover from a clone, use **mminfo** to determine the clone pool, then specify the pool name in the **recover** command.

### Procedure

- Use **mminfo** to determine the clone pool that contains the clone save set you want to recover:

```
mminfo -r volume, savetime, client, ssid, cloneid, name
```

volume	date	client	pool	name
backup.001	05/03/2013	bu_iddnwserver	Default	C:\ddlib
clone.001	05/03/2013	bu_iddnwserver	Default Clone	C:\ddlib

- Specify the clone date and clone pool in the **recover** command.

For example:

```
recover -t 05/03/2013 -b "Default Clone"
```

- Recover the data.

## Recovering a save set when all cloned instances have expired

When all cloned instances of a save set have passed their retention period, the following procedure must be used to mark a save set as eligible for recovery:

### Procedure

- Use the **nsrmm** command with the **-e** time option to change the retention time for the clone save set:

```
nsrmm -e time -S ssid/cloneid
```

If the cloneid is not identified with the **-S** option, the following error message is displayed:

```
Save set ssid cannot be marked as notrecyclable. Please specify the ssid/cloneid of the particular clone instance.
```

- Use the **nsrmm** command with the **-o notrecyclable** option to instruct the media database that the save set is no longer expired:

```
nsrmm -o notrecyclable -S ssid/cloneid
```

If the `-o notrecyclable` option is used with nsrmm prior to changing the retention time, the following error message is displayed:

```
nsrmm: Save set ssid:ssid cloneid:cloneid eligibility cannot be cleared, retention time must be adjusted first
```

After this procedure has been completed, the save set is recoverable.

## Cloning archived data

You can schedule a clone job to clone archive data or clone archive data on-demand.

### Setting up a scheduled clone job

#### Procedure

1. From the **Administration** window, click **Configuration**.
2. In the expanded left pane, select **Clones**.
3. From the **File** menu, select **New**.
4. In the **Name** attribute, type a unique name to identify the scheduled clone resource. Type additional information in the **Comment** attribute if necessary.
5. If you wish to override the saveset's original browse and retention policies, select new policies in the **Browse** and **Retention** policies attributes.
6. To specify the storage node that will write data during the clone operation, select a storage node from the **Storage node to WRITE save sets attribute**. If a selection is made in this attribute, it will override any storage node selection criteria.

This attribute is used primarily in conjunction with the Storage node to READ save sets attribute to balance access to storage media across different storage nodes.

7. To specify the storage node that will read data during the clone operation, select a storage node value from the **Storage node to READ save sets attribute**. This attribute is visible only when Diagnostic mode is selected. Additionally, the selected storage node must be included in at least one of the following:
  - The **Recover storage nodes** or **Storage nodes** attribute of the NetWorker server's client resource.
  - The storage node listed in the **Read Hostname** attribute for the library resource, if a library is being used.
  - A storage node on which any device in the library is configured, if a library is being used.

This attribute is used primarily in conjunction with the Storage node to WRITE save sets attribute to balance access to storage media across different storage nodes and is not intended for use with standalone devices such as AFTD's, file type devices, Data Domain devices, and so on.

8. To specify the clone media pool to write data to during a clone operation, select a clone type media pool from the **Write clone data to pool** attribute. If no selection is made, clones will be written to the default clone pool.

Pools are used to direct backups to specific media volumes. This attribute is particularly useful when you want to ensure that only certain media types are used to hold clone data. For example, to ensure that this clone job only replicates to a certain type of disk, such as a Data Domain type disk, select a clone pool that uses only Data Domain type disks. Likewise, to ensure that this clone job only replicates to tape (tape out), select a clone pool that uses only tape devices.

9. Select **Continue on save set error** to force NetWorker to skip invalid save sets and to continue the clone operation. If this option is not selected (default setting), an error message will be generated and the clone operation will not continue if an invalid save set or invalid volume identifier is encountered.

10. To restrict the number of clone instances that can be created for any save set that is included in this particular scheduled clone operation, type a value in the **Limit number of save set clones** attribute. A value of zero (0) means that an unlimited number of clones may be created for this scheduled clone operation.

Consider limiting the number of save set clones in cases where the clone operation has not completed and is being retried. For example, if you type a value of 1 in this attribute and then retry a partially completed clone operation, only the save sets that were not successfully cloned the first time will be eligible for cloning. In this way, unnecessary clone instances will not be created.

Regardless of the value in this attribute, NetWorker always limits the number of save set clone instances to one per volume. A clone pool can have multiple volumes. This attribute limits the number of save set clone instances that can be created for a clone pool in a particular scheduled clone operation.

11. Select **Enable** to allow the clone job to run at its scheduled time.

12. In the **Start Time** attribute, click the up and down arrows to select the time to start the clone job. Alternatively, type the time directly into the attribute fields.

13. From the **Schedule Period** attribute, select **Weekly by day** or **Monthly by day** depending on how you want to schedule the clone job and then select the day(s) of the week or month on which the scheduled clone is to occur.

14. To repeat the clone job within a day, specify an **Interval** time in hours. For example, if the start time is **6 AM**, and the interval is 6 hours, then the clone job will run at 6 AM, 12 PM, and 6 PM.

If the Limit the number of save set clones value is set, then the repeat clone job will fail after the limit is reached.

15. Select the **Save Set Filters** tab to specify the save sets to be included in this scheduled clone job.

16. Select **Clone save sets that match selections** to limit save sets by various filter criteria or select **Clone specific save sets** to explicitly identify the save sets to be cloned.

To clone save sets that match selection criteria:

- Specify selection criteria to limit the save sets that will be included in this scheduled job. You can select the following criteria:
  - Groups (save groups), required for snapshot rollover clones.
  - Clients (client resources)
  - Pools (backup pools),  
select an archive pool for archive data.
  - Filter save sets by level (backup level)
  - Filter save sets by name (save set name as specified in the Client resource)
  - Include save sets from the previous (save sets from the past number of days, weeks, months, or years)  
To display a list of the save sets that will be cloned based on the filter criteria that you specified, select **Preview Save Set Selection**.

To clone specific save sets:

- Type the specific save set ID/clone ID (ssid/clonid) identifiers in the **Clone specific save sets** list box. Type each ssid/cloneid value on a separate line.

You can query save set IDs / clone IDs through the **Administration > Media** user interface, or by using the `mminfo` command.

17. Select **OK** to save the scheduled clone job.

## Cloning archive volumes on-demand

### Procedure

1. From the **Administration** window, click **Media**.
2. In the expanded left pane, select **Save Sets**.
3. In the right pane, select the **Query Save Set** tab.
4. In the **Pool** attribute, select an archive pool from the list. Make other selections, as appropriate, to limit the save set search criteria.
5. Click the **Save Set List** tab.
6. Select the archive save sets to clone from the **Save Set** list.
7. From the **Media** menu, select **Clone**.
8. From the **Target Clone Media Pool** list, select an archive clone pool.
9. Click **OK** and then click **Yes** on the confirmation screen.

## Directing clones to a special storage node

You can direct clone operations to a specific storage node. This section describes the criteria used to determine the storage node from which the clone data is read (read source) and the storage node to which the clone data is written (write source).

### Storage node selection criteria for reading the clone data

The following logic is used to determine the storage node from which the clone data will be read (read source):

1. If the source volume is mounted, then the storage node of the device on which the volume is mounted is used as the read source.
  - If the `FORCE_REC_AFFINITY` environment variable is set to **Yes**, the selection criteria is ignored and the selection criteria behaves as though the volume is not mounted.
  - When cloning is used in a Virtual Tape Library (VTL) environment such as a CLARiiON Disk Library (CDL), the NetWorker software behaves as if the `FORCE_REC_AFFINITY` environment variable is set to **Yes**.
2. If the volume is not mounted or if the `FORCE_REC_AFFINITY` environment variable is set to **Yes**, a list of eligible storage nodes is created. The list is based on the storage nodes that meet both of the following criteria:
  - a. The storage nodes listed in the **Recover Storage Nodes** attribute of the NetWorker server's client resource. If this attribute is empty, the clone operation uses the following logic to choose the read device:
    - If the Autoselect storage node is not enabled in the client resource for the NetWorker server, then the clone operation will use the value in the NetWorker server's **Storage Nodes** attribute.
    - If the Autoselect storage node option is enabled in the client resource for the NetWorker server, then the clone operation will use the autoselect logic to choose the storage node.

- b. If the requested volume is in a media library, the storage nodes on which the volume can be mounted are determined in the following manner:
  - The storage node listed in the Read Hostname attribute for the library resource is used.
  - If the Read Hostname attribute for the library resource is not set, then all storage nodes on which any device in the library is configured is added to the list of eligible storage nodes.
  - If the volume is not in a media library, then the list of storage nodes is based on the criteria for storage nodes listed in the Recover Storage Nodes Attribute only.

### Selecting a storage node read source example

In this example, the volume resides in a media library and is not mounted. The Recover Storage Nodes attribute in the NetWorker server's Client resource lists the following storage nodes in order:

- Storage node F
- Storage node E
- Storage node D

The Read Hostname attribute for the library resource is not set, however, the following devices in the media library are configured with storage nodes:

- Device A is configured on storage node D
- Device B is configured on storage node E
- Device C is configured on storage node B

The list of eligible storage nodes is the intersection of the two previous lists. Therefore the list of eligible storage nodes is as follows:

- Storage node E
- Storage node D

The order in which the storage node is selected is based on the order of the Recover Storage Node attribute list. In this example, storage node E is selected first as the read source storage node. If storage node E is not available, then storage node D is selected.

In this example, if no matching storage nodes were found in the intersecting list, an error would be written to the daemon log file that indicates no matching devices are available for the operation. To correct the problem, make adjustments so that at least one matching storage node can be found in both lists.

### Storage node selection criteria and settings for writing a clone

The following priorities determine which storage node will store the cloned backup data. The storage node where the backup data resides is called the "read source." The storage node that stores the cloned data is called the "write source":

1. The read source storage node specifies the write source in its **Clone Storage Nodes** attribute.
2. If this attribute is blank, then the NetWorker server's storage node specifies the write source in its **Clone Storage Nodes** attribute.
3. If this attribute is empty, the clone operation uses the following logic to choose the write device:

- If the **Autoselect storage node** is not enabled in the client resource for the NetWorker server, then the clone operation will use the value in the NetWorker server's **Storage Nodes** attribute.
- If the **Autoselect storage node** option is enabled in the client resource for the NetWorker server, then the clone operation will use the autoselect logic to choose the storage node.

Wherever the cloned data is written, the client file index and media database entries for the cloned save sets will reside on the NetWorker server.

## Specifying a clone from a volume shared by multiple devices

In backup-to-disk environments it is possible for a single backup volume to be shared by multiple storage devices on different storage nodes. The **Clone Storage Nodes** attribute on each of these storage nodes can specify a different clone write source. Thus the write source for data cloned from the backup volume can be ambiguous depending on which device reads the volume.

To ensure unambiguous clone write sources in this situation, configure the **Clone Storage Nodes** attribute of all the storage nodes that have access to the backup volume to specify the same storage node write source.

## Cloning from one storage node to another

### Procedure

1. In NMC, connect to the NetWorker server.
2. In the **Devices** view, select **Storage Nodes** in the navigation tree.
3. Right-mouse click the storage node where the backup data resides (read source storage node) and select **Properties**.
4. On the **Configuration** tab, in the **Clone Storage Nodes** attribute, type the hostname of the storage node that will store the cloned backup data.

## Cloning from many storage nodes to one storage node

### Procedure

1. In NMC, connect to the NetWorker server.
2. In the **Devices** view, select **Storage Nodes** in the navigation tree.
3. Right-mouse click the NetWorker server's Storage Node resource and select **Properties**.
4. On the **Configuration** tab, in the **Clone Storage Nodes** attribute, type the hostname of the storage node that will store all the cloned backup data.
5. Configure each read source Storage Node resource to ensure that the **Clone Storage Nodes** attribute is blank.

## Storage node selection criteria for recovering cloned data

The following logic is used to determine the storage node from which the clone data will be recovered:

1. If the source volume is mounted, then the storage node of the device on which the volume is mounted is used as the read source.  
If the **FORCE\_REC\_AFFINITY** environment variable is set to Yes, the selection criteria is ignored and the selection criteria behaves as though the volume is not mounted.

When cloning is used in a Virtual Tape Library (VTL) environment such as a CLARiiON Disk Library (CDL), the NetWorker software behaves as if the FORCE\_REC\_AFFINITY environment variable is set to Yes.

2. If the volume is not mounted or if the FORCE\_REC\_AFFINITY environment variable is set to Yes, a list of eligible storage nodes is created. The list is based on the storage nodes that meet both of the following criteria:
  - a. The storage nodes listed in the **Recover Storage Nodes** attribute of the NetWorker client resource that is being recovered. If this attribute is empty, NetWorker will use the following logic to choose the read device:
    - If the Autoselect storage node is not enabled in the client resource for the NetWorker server, then the recovery operation will use the value in the NetWorker server's Storage Nodes attribute.
    - If the Autoselect storage node option is enabled in the client resource for the NetWorker server, then the recovery operation will use the autoselect logic to choose the storage node.
  - b. If the requested volume is in a media library, the storage nodes on which the volume can be mounted are determined in the following manner:
    - The storage node listed in the Read Hostname attribute for the library resource is used.
    - If the Read Hostname attribute for the library resource is not set, then all storage nodes on which any device in the library is configured is added to the list of eligible storage nodes.
    - If the volume is not in a media library, then the list of storage nodes is based on the criteria for storage nodes listed in the Recover Storage Nodes attribute only.

## Using file type devices for clone operations

This section discusses issues related to cloning with file type and advanced file type devices.

### Differences in the cloning process

There are differences in the cloning process for the two types of devices:

- For file type devices, automatic and manual cloning begins only after all the save sets in a savegroup have been backed up.
- For advanced file type devices, automatic cloning begins only after all the save sets in a savegroup have been backed up. However, you can begin manually cloning a save set as soon as it has finished its backup.
- As of NetWorker 8.1, automatic cloning can begin after each save set in a savegroup is backed up when using clone-controlled replication (CCR) with a DD Boost device.

### Manual cloning with advanced file type device

In a situation where there are three save sets:

- Save set A has a size of 10 KB
- Save set B has a size of 10 MB
- Save set C has a size of 10 GB

When save set A has completed its backup, you can begin the manual cloning process while the other two larger save sets are still being backed up.

As each save set is backed up, you can launch the cloning process for that save set.

You can only clone one save set at a time.

## Backup-to-tape for Avamar deduplication clients

The *EMC NetWorker Avamar Integration Guide* provides more information.

## Cloning with Data Domain devices

Data Domain devices were introduced in NetWorker 7.6 Service Pack 1 and enable one to perform clone controlled replication (optimized cloning) from one Data Domain device to another. You can also clone to tape or to any other device type.

Clone operations with Data Domain devices are set up in basically the same way as any other scheduled clone operation. However, there are some special considerations to be aware of when setting up Data Domain devices. These are described in the *EMC NetWorker Data Domain Devices Integration Guide*.

## Using the nsrclone command

As of NetWorker 7.5, the `nsrclone` command has been enhanced to provide greater flexibility in selecting save sets for cloning by clients, groups, save set names, save set levels, and by number of valid copies or clones not yet created in the target pool. Also, be aware that as of NetWorker 7.6 Service Pack 1, most of the functionality provided in the `nsrclone` command is now provided in the Clone resource user interface.

The following table provides the descriptions of the new options available in NetWorker 7.5 and later, that can be used with the `nsrclone` command.

**Table 50** List of `nsrclone` options and their descriptions

Options	Description
<code>-C</code> less than copies in target pool	Specifies the upper non-inclusive integer limit such that only save sets with a lesser number of clone copies in the target clone pool are considered for cloning. This option is useful when retrying aborted clone operations. Because the target is a clone pool, each save set's original copy or clone is never considered when counting the number of copies of the save set. Likewise, any AFTD read-only mirror clone is not considered because its read or write master clone is counted and there is only one physical clone copy between the related clone pair. Recyclable, aborted, incomplete and unusable save set or clones are excluded in the counting. This option can only be used with the <code>-t</code> or <code>-e</code> option.
<code>-l</code> level or range	Specifies the level or <code>n1-n2</code> integer range from 0 to 9 for save sets that are considered for cloning. Manual for ad-hoc or client-initiated save sets, full for level full save sets, incr for level incremental save sets, and integers 0 through 9, where save set 0 also means full, can be used. More than one level can be specified by using multiple <code>-l</code> options and the <code>-l n1-n2</code> range format. This option can only be used with the <code>-t</code> or <code>-e</code> option.

**Table 50** List of nsrclone options and their descriptions (continued)

Options	Description
-N save set name	Specifies the save set name for save sets that are considered for cloning. More than one save set name can be specified by using multiple -N options. This option can only be used with the -t or -e option.
-c client name	Specifies the save sets in the particular client. More than one client name can be specified by using multiple -c options. This option can only be used with the -t or -e option.
-g group name	Specifies the save sets in the particular group. More than one group name can be specified by using multiple -g options. This option can only be used with the -t or -e option.

## nsrclone option examples

The following examples show how various options can be used with the `nsrclone` command:

Copy all save sets created in the last twenty-four hours for clients mars and jupiter with save set names /data1 and /data2 for only backup level full:

```
nsrclone -S -e now -c mars -c jupiter -N /data1 -N /data2 -l full
```

Copy all save sets that were not copied to the default clone pool in a prior partially aborted nsrclone session:

```
nsrclone -S -e now -C 1
```

Copy all save sets that were not copied to the default clone pool in a previous partially aborted nsrclone session and with extended retention and browse periods:

```
nsrclone -S -e now -C 1 -y 12/12/2010 -w 12/12/2009
```



# CHAPTER 13

## Staging Backups

This chapter contains the following topics:

- [Save set staging](#).....342
- [Working with staging policies](#).....342

## Save set staging

Save set staging is the process of transferring data from one storage medium to another medium, and then removing the data from its original location. For example, the initial backup data can be directed to a high performance file type or advanced file type device. In this way, the backup time is reduced by taking advantage of a file or advanced file type device. At a later time, outside of the regular backup period, the data can be moved to a less expensive but more permanent storage medium, such as magnetic tape. After the backup data is moved, the initial backup data can be deleted from the file or advanced file type device so that sufficient disk space is available for the next backup.

A save set can be staged from one disk to another as many times as required. For example a save set could be staged from disk 1, to disk 2, to disk 3, and finally to a remote tape device or cloud device. Once the save set is staged to a tape or cloud device, it cannot be staged again. However, you could still clone the tape or cloud volume.

Staging can be driven by any of the following:

- Calendar-based process, such as keeping the save set for 30 days on the staging device before moving the data to the next device.
- Event-based process, such as when available space in the staging pool drops below a set threshold. When this happens, the oldest save sets are moved until available space reaches a preset upper threshold.
- Administrator-based process, such as allowing the administrator to either reset the threshold or manually select save sets to stage.

Staging does not affect the retention policy of backup data. Therefore, staged data is still available for recovery.

When the nsrstage process encounters an error after successfully cloning specified save sets, it deletes only those successful save sets from the source volume before the program is aborted. This ensures that only a single set of save sets exist in either of the source or clone volumes after staging.

## Working with staging policies

This section describes how to work with staging policies.

[Backup to Disk and Cloud on page 151](#) [Backup to Disk and Cloud on page 151](#) provides information on disk based device configuration.

### Creating a staging policy

Before creating a staging policy configure all appropriate devices. Otherwise, no devices will be listed in the Devices attribute.

To prevent an advanced file type device from becoming full during backup, the staging policy must be set up so that save sets are automatically moved to another medium to make disk space available in the advanced file type device.

#### Procedure

1. In the **Administration** window, click **Configuration**.
2. In the left pane, select **Staging**.
3. From the **File** menu, select **New**.
4. In the **Name** attribute, type a name for the staging policy.

5. In the **Comment** attribute, type a description of the staging policy.
6. To enable staging to begin immediately or to be invoked automatically at a later time, set the **Enabled** attribute to **Yes**.

You can enable or disable staging at any time.

7. In the **Devices** attribute, select the file type and adv\_file type devices as the source device for staging. You can assign multiple devices to the staging policy, but a given device cannot be controlled by more than one staging policy.
8. For the **Destination Pool** attribute, select the destination pool for the staged data.

If the Clone pool you have selected is restricted to storage node devices, you will also need to modify Clone Storage Nodes attribute of the Storage Node resource for the NetWorker server to include the storage node name.

[Storage node selection criteria and settings for writing a clone on page 335](#) provides details.

9. In the **High-Water Mark (%)** attribute, type or select a number.

This value is the point at which save sets should be staged, measured as the percentage of available space used on the file system partition that the file device is on. Staging continues until the low-water mark is reached.

The high-water mark must be greater than the low-water mark.

10. In the **Low-Water Mark (%)** attribute, type or select a number. This is the point at which the staging process will stop, measured as the percentage of available space on the file system partition that the file device is on.
11. From the **Save Set Selection** attribute, select from the list to determine the save set selection criteria for staging.
12. In the **Max Storage Period** attribute, type the number of hours or days for a save set to be in a volume before it is staged to a different storage medium.

The Max Storage Period attribute is used in conjunction with the File System Check Interval attribute. Once the Max Storage Period value is reached, staging does not begin until the next file system check.

13. In the **Max Storage Period Unit** attribute, select **Hours or Days**.

14. In the **Recover Space Interval** attribute, type the number of minutes or hours between recover space operations for save sets with no entries in the media database from file or advanced file type devices.

15. In the **Recover Space Interval Unit** attribute, select **Minutes or Hours**.

16. In the **File System Check Interval** attribute, type the number of minutes or hours between file system checks.

At every File System Check interval, if either the High-Water Mark or Max Storage Period has been reached, a staging operation is initiated.

17. In the **File System Check Interval Unit** attribute, select **Minutes or Hours**.

18. To invoke the staging policy immediately, complete this step. Otherwise, skip this step.
  - a. Select the **Operation > s** tab.
  - b. In the **Start Now** attribute, select one of these operations:
    - Recover space — Recovers space for save sets that have no entries in the media database and deletes all recycled save sets.
    - Check file system — Checks file system and stage data, if necessary.

- Stage all save sets — Stages all save sets to the destination pool. The selected operation applies to all devices associated with this policy. The choice you make takes effect immediately after clicking OK. After the staging operation is complete, this attribute returns to the default setting (blank).

19. When all the staging attributes are configured, click **OK**.

## Errors with device usage statistics when staging and backup operations are concurrent

When disk devices such as AFTDs perform staging and backup operations concurrently, NetWorker does not accurately display the disk volume's usage total. The inaccurate data can be seen in the Written column when using the `mminfo -mv` report command or in the Used column when viewing volume information in the Media window of the NetWorker Administration application.

## Editing a staging policy

### Procedure

1. In the **Administration** window, click **Configuration**.
2. In the left pane, select **Staging**.

3. In the right pane, select the **Staging** policy to edit.

You cannot edit the name of an existing staging policy.

4. From the **File** menu, select **Properties**.
5. Make any necessary changes and click **OK**.

## Copying a staging resource

### Procedure

1. In the **Administration** window, click **Configuration**.
2. In the left pane, select **Staging**.
3. In the right pane, select the **Staging** resource to copy.
4. From the **Edit** menu, select **Copy**. The **Create Staging** dialog box appears, containing the same information as the Staging resource that was copied, except for Name attribute.
5. Type the name for the new **Staging** resource in the Name attribute, edit any other attributes as appropriate, and click **OK**.

## Deleting a staging policy

The Default staging policy cannot be deleted.

### Procedure

1. In the **Administration** window, click **Configuration**.
2. In the left pane, select **Staging**.
3. Remove all devices from the **Staging** policy.
  - a. In the right pane, select the **Staging** policy to be deleted.
  - b. From the **File** menu, select **Properties**.
  - c. In the **Devices** attribute, ensure that all listed devices are unselected.

- d. Click **OK**.
- 4. In the right pane, select the **Staging** policy to be deleted.
- 5. From the **File** menu, select **Delete**.
- 6. When prompted, click **Yes** to confirm the deletion.

## Consideration for staging a bootstrap backup

Bootstrap backups can be directed to a disk device such as an AFTD or FTD device. However, if a bootstrap backup is staged to another device, the staging operation will complete and will be reported as complete even though the “recover space” operation will not be executed. This means that the staged bootstrap will remain on the original disk from which it was staged. Therefore, the original disk can be used to scan in the bootstrap data if the staged bootstrap is accidentally deleted. Also be aware that if the bootstrap data is not staged from the original disk, the data on the original disk will be subject to the same browse and retention policies as any other save set backup and will, therefore, be subject to deletion after the retention policy has expired.

## Staging and cloning from the command prompt

Staging a save set from the command prompt works differently than staging a save set from the NetWorker Console. When staging from the NetWorker Console, you select save sets that belong to a single device. When staging from the command prompt, specify the save set IDs to be staged.

When a save set is cloned, the cloned save sets are given the same save set ID as the original save set with a new clone ID. When staging a save set from the command prompt, the NetWorker software stages all the save sets with the specified save set ID and then removes those save sets. That means that any cloned versions of the save set are removed when the original is removed.

To ensure that all clones are not removed, specify a clone ID with the save set ID to indicate the source volume of the staging. For example:

```
nsrstage -m -S ssid/cloneid
```

To find the clone ID of a save set, use the `mminfo` command. For example:

```
mminfo -avot -r "volume,ssid,cloneid,name"
```

For information about `nsrstage` or `mminfo`, refer to the *EMC NetWorker Command Reference Guide* or the UNIX man pages.

## Staging Backups

# CHAPTER 14

## Recovering Filesystem Data

This chapter contains the following topics:

• <a href="#">NetWorker recovery overview</a> .....	348
• <a href="#">Overview of NetWorker recovery methods</a> .....	351
• <a href="#">Recovering the data</a> .....	352
• <a href="#">Recovering deduplication data</a> .....	367
• <a href="#">Recovering with BMR</a> .....	367
• <a href="#">Recovering ACL files</a> .....	367
• <a href="#">Recovering encrypted data</a> .....	367
• <a href="#">Recovering Windows volume mount points</a> .....	368
• <a href="#">Recovering special Windows databases</a> .....	369
• <a href="#">Recovering expired save sets</a> .....	369
• <a href="#">Recovering client files on a different NetWorker server</a> .....	374
• <a href="#">Recovering critical NetWorker server databases</a> .....	376
• <a href="#">Recovering the NMC server database</a> .....	387

## NetWorker recovery overview

You can recover NetWorker data by using the recover command, the NetWorker User program on Windows, or the NMC Recovery wizard on the NMC server.

The NetWorker User and the NMC Recovery Wizard programs recover data sequentially. You can use multiple recover commands to recover files in parallel.

Three types of NetWorker hosts are involved in a recovery operation:

- Administering host—The NetWorker host that starts the recovery.
- Source host—The NetWorker host from which the backup was run.
- Destination host—The NetWorker host that receives the recover data.

Perform a recovery operation in one of two ways:

- Local recover—A single NetWorker host is the administering, source and, destination host.
- Directed recover—The administering host is the source host or any other NetWorker host in the datazone. The destination host is not the source host.

Use a directed recovery:

- To centralize the administration of recoveries from a single host.
- To recover the data to a shared server, when the user cannot recover the data themselves.
- To recover data to another host because the source host is inoperable or the network does not recognize the source host.
- To transfer files between two NetWorker hosts. For example, if the AUTOEXEC.BAT or .profile file on a client is appropriate for a new client, recover the file to the new client.

## Local recoveries

In a local recovery, the administering host is also the source and destination host. Local recoveries are the simplest way to recover NetWorker data.

To perform a local recovery, the user on the local host, user@localhost must:

- Belong to a NetWorker User Group that has the Recover Local Data privilege. The EMC NetWorker Security Configuration Guide provides more information.
- Have operating system ownership of the recovered files. The root user on UNIX and the Windows Administrator have this privilege.
- Have write privileges to the local destination directories. The root user on UNIX and the Windows Administrator have this privilege.

## Directed recoveries

A directed recovery enables a NetWorker administrator to recover data to a NetWorker host that differs from the source of the backup, while retaining the original file ownership and permissions.

A directed recovery is a restricted NetWorker function available only to user accounts that have the necessary privileges required to perform the operation.

A user with directed recovery privileges can:

- Browse the backup data of all NetWorker clients.

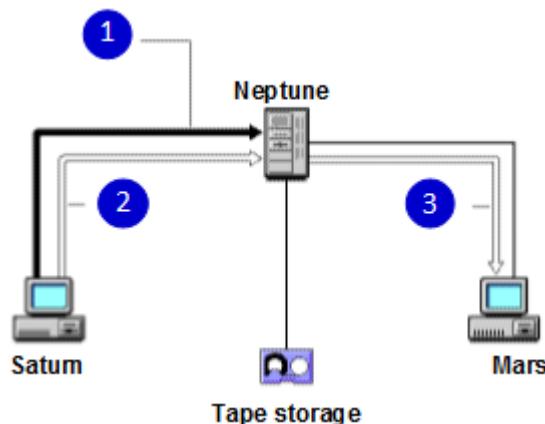
- Recover the data to any NetWorker client.

This figure provides an example of a directed recovery. A user on the client Saturn (administering client) performs a directed recovery of data from a remote client to Mars (destination client). The OS of the destination client must match that of remote client. Neptune is the NetWorker sever. The Tape Storage contains backups from a remote client.

In this figure, the numbers represent the following:

1. Saturn requests to browse backups from a remote client (not shown)
2. Request to recover data from tape storage to client Mars
3. Data recovered to client Mars

**Figure 29** A directed recovery from a remote client



## Directed recover requirements

The following table summarizes recover requirements for each host in a recover session.

**Table 51** General recover requirements

Host	Requirements
Destination	<p>Is the same platform as the source host, for example, UNIX to UNIX or Windows to Windows.</p> <p>Uses the same file system as the source host, for example, UXFS to UXFS or NTFS to NTFS.</p> <p>The root user or the Administrator user on the destination host must be one of the following:</p> <ul style="list-style-type: none"> <li>• A member of a NetWorker User Group with Remote Access All Clients privileges.</li> <li>• Added to the Remote Access attribute of the source host. For example: The source client is mars. The destination client venus, is a Windows host. The Remote Access attribute for the client mars contains: <code>Administrator@venus</code></li> </ul> <p>The servers file contains an entry for the administering host. The <i>NetWorker Security Configuration Guide</i> provides more information about client-tasking rights and how to modify the servers file.</p> <p>The Disable Directed Recover attribute is set to the default value No, in the NSRLA database. A value of No means that the client accepts directed</p>

**Table 51** General recover requirements (continued)

Host	Requirements
	recoveries from remote hosts. <a href="#">Editing a client NSRLA database on page 530</a> describes how to edit the NSRLA database.
Source	<p>The same platform as the destination host, for example, UNIX to UNIX or Windows to Windows.</p> <p>Uses the same file system as the destination host, for example, UXFS to UXFS or NTFS to NTFS.</p> <p>The Remote Access attribute contains the user account of the administering host. For example:</p> <p>The source client is mars and the administering client is venus. The Administrator account on venus starts the recover program. The value in the Remote Access attribute for the client mars is:</p> <p>Administrator@venus</p>
Administering	<p>A client of the NetWorker server that contains the backup information. The administering client can be a different platform from the source and destination clients.</p> <p>Use the local root or Administrator account to start the recover. Ensure the user account is a member of one of the following:</p> <ul style="list-style-type: none"> <li>• The Operators, the Application Administrators, the Database Administrators, or the Database Operators User Group. You must have operator privileges in the Operators user group to perform a selective files restore from a Microsoft Windows deduplication backup. Microsoft provides complete documentation for working with the Windows deduplication functionality.</li> <li>• A customized User Group with the following privileges on the NetWorker server: Remote Access All Clients Operate NetWorker Monitor NetWorker Operate Devices and Jukeboxes Backup Local Data Recover Local Data Recover Remote Data <a href="#">Managing server access on page 494</a> provides more information about access requirements</li> </ul>
Virtual cluster client	A Client resource for the virtual cluster client must exist on the NetWorker server. The Remote Access attribute for the virtual cluster client must contain an entry for the root or Administrator user for each physical cluster node.

## Windows requirements

Review this section before you perform a directed recovery of a Windows client:

- You cannot recover data from a backup that you performed on a NetWorker 8.1 or higher client to a pre-NetWorker 8.1 client.

- You cannot perform a directed recovery to a CIFS share.
- Enable the Windows File and Print Sharing option on a Windows destination client.
- If you use the recover command and the NetWorker server and clients are Microsoft Windows hosts, then:
  - When the NetWorker server and the destination host are in the same domain, start the **NetWorker Backup and Recovery** service with a domain user that is a member of the local Administrators group.
  - When the NetWorker server and destination host are not in a domain, or are not in the same domain, start the NetWorker Backup and Recovery service with a local user that exists on both hosts. The local user must have the same password on both hosts and be a member of the local Administrators group on the NetWorker server.

## UNIX specific requirements

When relocating non-ASCII directories on UNIX hosts:

- If the remote directory is an existing non-ASCII directory, the locale of the administering client must match the locale of the destination client.
- If the remote directory does not exist, NetWorker creates the relocation directory on the destination file system, based on the locale of the administering client.

# Overview of NetWorker recovery methods

Determine the recovery method that you will use:

- [Browsable recovery on page 351](#)
- [Save set recovery on page 352](#)
- [Scanner recovery on page 352](#)
- [VSS File Level Recovery on page 352](#)

## Browsable recovery

The file selection recovery method, or browsable recovery enables you to browse for and select the files and directories to recover. The browse policy applied at the time of backup determines the earliest versions of files and file systems that are available for recovery. [About browse and retention policies on page 232](#) provides more information about browse policies.

Use a file selection recovery when:

- You do not know the exact name of the file or directory to recover.
- You want to recover a small number of files or directories. When you select many files and directories, the recover process can take some time to complete, particularly from the NetWorker User program.
- You want to perform a directed recovery.
- You want to recover only the files that you select, not extra files.

## Save set recovery

The save set selection recovery method, or save set recover enables you to recover data without browsing and selecting the files for recovery. Unlike a browsable recovery, a save set recover does not inspect the client file index for information about each selected file.

When you perform a save set recover, recover the last full backup first, then recover levels 1 to 9 and incremental backups in the chronological backup order. [Backup levels on page 263](#) provides information about the relationship between full backups, backup levels 1 to 9, and incremental backups.

Use a save set recovery when:

- You want to recover many files or all the data in a save set, for example, in the event of a total disk failure. When you perform a save set recovery, you do not select individual files or directories for recovery.
- You want to recover data from a recoverable or recyclable save set. [About browse and retention policies on page 232](#) provides more information about browse and retention policies. [Recovering a recyclable or recoverable save set entry in the online indexes on page 370](#) describes how to repopulate the client file index entries for recoverable and recyclable (expired) save sets.
- Memory resources on the recovery host is scarce. A save set recovery requires less memory than a browseable recovery.

## Scanner recovery

The `scanner` program enables you to recover data directly from a volume

Use the `scanner` program to recover data when:

- You want to perform a by file selection recovery but the save set information is not in the client file index.
- You want to recover data directly from a tape.
- You want to recover data from an incomplete save set.

## VSS File Level Recovery

VSS File Level Recovery (FLR) provides the ability to browse, select and restore any System State file from the backup of the volume where it resides. There are changes to how Windows VSS-based backups and restores behave. The major changes include:

- System state files are now backed up as part of the volumes where they reside.
- All file system backups require that all system writers affected by the backed up volumes be included to ensure the backups are VSS consistent. You can use the command line flag `VSS:=off`, to remove this VSS requirement.
- The Exclude file list specified by system state writers, and directives specified by unsupported application writers continue to work and are excluded from file system backups.

## Recovering the data

NetWorker provides four applications to recover data. The application that you can use to recover data depends on the administrative host used to recover the data.

To perform recoveries:

- From the NMC server, use the NMC Recovery Wizard. [Using the Recovery Wizard on page 353](#) provides more information.
- From a command prompt, use the recover command. [Using the recover command on page 358](#) provides more information.
- From a Windows administrative host, use the NetWorker User application. [Using the NetWorker User program on page 361](#) provides more information.
- From the NetWorker server when save set information is not in the media database, use the scanner command. [Using the scanner program to recover data on page 365](#) provides more information.
- [Using VSS file level recovery \(FLR\) on page 366](#) provides information on recovering data by using VSS FLR.

## Using the Recovery Wizard

NetWorker includes a new Recovery Wizard that allows you to recover data to NetWorker 8.1 and later clients from a centralized location, the NMC GUI. The Recovery Wizard supports browsable, save set, and directed recoveries. The Recovery Wizard does not support cross-platform recoveries.

Use the Recovery Wizard to configure scheduled and immediate recoveries of:

- File system backups.
- NDMP backups, when you use a NetWorker server 8.1.1 or later and NMC server 8.1.1 or later.

---

### Note

When you use NetWorker server 8.1 and earlier, the Recovery Wizard does not display NDMP clients in the Select Recovery Hosts window.

- Block Based Backups (BBB).
- BBB that you cloned to tape.

You can also use the Recovery wizard to configure an immediate recover of a Snapshot Management backup.

When you create a recover configuration by using the Recovery Wizard, NetWorker saves the configuration information in an NSR recover resource in the resource database of the NetWorker server. NetWorker uses the information in the NSR recover resource to perform the recover job operation.

When a recover job operation starts, NetWorker stores:

- Details about the job in the nsrjobsd database. [Using nsrrecomp on page 464](#) describes how to query and report on recovery status.
- Output sent to stderr and stdout in a recover log file. NetWorker creates one log file for each recover job. [Troubleshooting Recovery Wizard on page 355](#) provides more information.

---

### NOTICE

NetWorker removes the recover log file and the job information from the job database based on value of the Jobsdb retention in hours attribute in the properties of the NetWorker server resource.

## Recovery Wizard requirements

Review this section before you use the Recovery Wizard.

Ensure that:

- The destination host is a client of the NetWorker server.
  - For a directed recover, the Remote Access attribute of the source client must contain the hostname of the destination client.
  - The source and destination clients are running the NetWorker 8.1 or later software.
- 

### Note

You can recover data from a pre-8.1 backup after you update the source host to NetWorker 8.1 or later.

- The account you use to connect to the Console server has Configure NetWorker privileges. The EMC NetWorker Security Configuration Guide provides more information.
- The appropriate configuration is in place if you will perform a directed recover. [Directed recoveries on page 348](#) provides more information.

## Creating a new recover configuration

The Recovery Wizard allows you to create and save a configuration that you can reuse or modify later.

### Procedure

1. Use NMC to connect to the NetWorker server.
2. Click **Configuration** from the left navigation pane, then select **Clients**.
3. Right-click the client from which you want to recover the data, then select **Recover**. The Recovery Wizard appears.
4. Navigate through the Recovery Wizard screens and define the configuration for the recover job. Online help describes how to use the Recovery Wizard.

## Modifying a saved recover configuration

The Recovery Wizard allows you to save partial recover configurations and complete the configuration at a later time.

### Procedure

1. Use NMC to the NetWorker server.
2. Click **Recover** on the Administration window toolbar. The **Recover** window appears. [Recover window on page 442](#) provides more information about the Recover window.
3. In the **Configured recovers** window, right-click the saved recover configuration, select **Open Recover**.

## Reusing recover configurations

When you define a recover configuration, the Recovery Wizard provides you with the option to save the recover configuration or delete the configuration after the recover

completes. When you save the configuration, you can reuse the configuration information to perform a new recover job.

### Before you begin

Connect to the NMC server from an NMC client. Ensure that the account you use to connect to the NMC server has Configure NetWorker privileges. The *EMC NetWorker Security Configuration Guide* provides more information.

### Procedure

1. Connect to the NetWorker server.
2. Click **Recover** on the **Administration** window toolbar. The **Recover** window appears. [Recover window on page 442](#) provides more information about the **Recover** window.
3. In the **Configured recovers** window, right-click the saved recover configuration, select **Recover Again**.
4. Make changes as required and save the configuration with a new name.

## Troubleshooting Recovery Wizard

At the start time for a Recovery resource, nsrd uses an nsrtask process on the NetWorker server to start the recover job. The nsrtask process requests that the nsrjobd process on the NetWorker server run the recovery job on the destination client, then nsrtask monitors the job.

Once the recover job starts:

- The log files on the NetWorker server contain stdout and stderr information for the recover job. NetWorker stores the logs files in the following location, by default:
  - Windows: C:\Program Files\EMC NetWorker\nsr\logs\recover
  - UNIX: /nsr/logs/recover

#### Note

NetWorker names the log file according to the name of the recover resource and the time of the recovery job: *recover\_resource\_name\_YYYYMMDDHHMMSS*

- The jobsdb contains job status information for the recover job.

## Debugging recover job failures from NMC

To troubleshoot a recovery issue by using NMC, configure the Recovery resource to display greater detail in the log file, then retry the recover configuration in debug mode:

### Procedure

1. In the **Recover** window, right-click the recover configuration and select **Recover Again**.
2. Click the **Back** button until you reach the **Select the Recover Options** window.
3. Select **Advanced Options**.
4. Increase the value in the **Debug level** attribute to enable debugging. The higher the value, the more the debug output that appears in the recover log file.
5. Click **Next** until you reach the **Perform the Recover** window.
6. In the **Recover name** field, provide a new name for the recover configuration.
7. Click **Run Recover**.
8. Monitor the status of the recover job in the option in the **Recover** window.

- When the recover completes, review the recover log file.

## Debugging recovery failures from command line

To troubleshoot recovery issue from the command line, use the **nsradmin** and **nsrtask** programs.

### Procedure

- From a command prompt on the NetWorker server, type **nsradmin**.
- From the **nsradmin** prompt:

- Set the resource attribute to the **Recover** resource. For example:

```
. type: nsr recover
```

- Display the attributes for the **Recover** resource that you want to troubleshoot. For example:

```
print name: recover_resource_name
```

Where *recover\_resource\_name* is the name of the Recover resource.

- Make note of the values in the **recover**, **recovery options**, and **recover stdin** attributes. for example:

```
recover command: recover;
recover options: -a -s nw_server.emc.com -c mnd.emc.com -I - -i
R;
recover stdin:
"<xml>
<browsetime>
May 30, 2013 4:49:57 PM GMT -0400
</browsetime>
<recoverpath>
C:
</recoverpath>
</xml>";
```

where:

- nw\_server.emc.com* is the name of the NetWorker server.
- mnd.emc.com* is the name of the source NetWorker client.

- To confirm that the **nsrd** process can schedule the recover job:

- Update the **Recover** resource to start the recover job:

```
update: name: recover_resource_name;start time: now
```

where *recover\_resource\_name* is the name of the Recover resource.

- Quit the **nsradmin** application.
- Confirm that the **nsrtask** process starts.
- If the **nsrtask** process does not start, the review the **daemon.raw** file on the NetWorker server for errors.
- To confirm that the NetWorker server can run the **recover** command on the remote host, type the following command on the NetWorker server:

```
nsrtask -D3 -t 'NSR Recover' recover_resource_name
```

Where *recover\_resource\_name* is the name of the Recover resource.

5. When the `nsrtask` command completes, review the `nsrtask` output for errors.
6. To confirm that the Recovery UI sends the correct recovery arguments to the `recover` process:
  - a. Open a command prompt on the destination client.
  - b. Run the `recover` command with the **recover options** that the Recover resource uses. For example:

```
recover -a -s nw_server.emc.com -c mnd_emc.com -I - -i R
```

- c. At the Recover prompt, specify the value in the **recover stdin** attribute.

---

**Note**

Do not include the “ ,”, or the ; that appears with the **recover stdin** attribute.

- d. If the `recover` command appears to hang, review the `daemon.raw` file for errors.
- e. When the `recover` command completes, review the `recover` output for errors. If the `recover` command fails, then review the values specified in the Recover resource for errors.
7. Use the `jobquery` command to review the details of the Recover job. From a command prompt on the NetWorker server, type: `jobquery`.
8. From the `jobquery` prompt, perform one of the following steps:

- a. To set the query to the Recovery resource and display the results of all recovery jobs for a Recovery resource, type:

```
print name: recover_resource_name
```

Where `recover_resource_name` is the name of the Recover resource.

- b. To set the query to a particular jobid and display the results of the job, type:

```
print job id: jobid
Where jobid is the jobid of the Recover job that you want to review.
```

---

**Note**

Review the `daemon.raw` file on the NetWorker server to obtain the jobid for the recovery operation.

## Common recovery error messages

This section contains a summary of common recovery error messages and resolutions.

### Unable to connect to the server. Remote system error - unknown error

This error appears in the **Select the Recovery Hosts** window when the Wizard cannot contact the host that you selected as the source or destination host.

To resolve this issue, ensure that:

- The host is powered on.
- The NetWorker Remote Exec service (`nsrexecd`) is started.
- Name resolution for the host is working correctly.

**Host *destination\_hostname* is missing from the remote access list of *source\_hostname*.**

**Press [Yes] to update the remote access list of *source\_hostname* with *destination\_hostname***

This message appears in the **Select the Recovery Hosts** window when you select a destination host that does not have the correct permissions to receive directed recovery data.

To resolve this issue, click **Yes**. The Recovery Wizard will update the Remote access attribute in the properties of the source host with the hostname of the destination host.

If you click **No**, then you cannot proceed in the recovery wizard until you select a destination host that is in the Remote access attribute of the source host.

**This host is either improperly configured or does not support this operation**

This message appears in the **Select the Recovery Hosts** window after you select a source or destination host when the source or destination host is running NetWorker 8.0 or earlier.

***Destination\_host\_name* does not support *recovery\_type***

This message appears in the **Select the Recovery Hosts** window after you select a destination host and the destination host does not support the recovery type that you selected. To resolve this issue, select a destination host that supports the recovery type.

## Using the recover command

Use the `recover` command to perform the data recovery from a command prompt.

There are two recovery methods:

- Interactive mode—enables the user on the administering host to browse and select files and directories from the source backup.
- Non-interactive mode—enables the user on the administering host to recover a directory or file immediately, without browsing the client file index for file information. Use non-interactive mode when you know the path to recover and do not need to browse through the backup data find it.

The following table provides information to review before performing a command line recovery.

**Table 52** Command line recovery considerations

When	Consider
Using <code>recover.exe</code> on Windows	<p>To avoid using the Windows version of <code>recover.exe</code> on Windows operating systems, perform one of the following:</p> <ul style="list-style-type: none"> <li>• Include <code>NetWorker_install_path\bin\recover.exe</code> at the command prompt</li> <li>• Ensure that <code>NetWorker_install_path\bin</code> appears before <code>%SystemRoot%\System32</code> in the <code>\$PATH</code> environment variable. To recover files or directories that begin with a dash (-) such as <code>-Accounting</code>, try one of the following options:</li> <li>• Run the <code>recover</code> command and type <code>add ./-Accounting</code> to recover the <code>-Accounting</code> file or directory and its contents.</li> </ul>

**Table 52** Command line recovery considerations (continued)

When	Consider
	<ul style="list-style-type: none"> <li>Run the <code>recover</code> command and use the <code>cd</code> command to change directories to <code>-Accounting</code>. Type <code>add .</code> to add the current directory and its contents for recovery.</li> <li>When the current directory is <code>/temp</code> and <code>-Accounting</code> resides in the <code>/temp</code> directory, run the <code>recover</code> command and type <code>add /temp/Accounting</code>. This adds <code>-Accounting</code> and the contents of the directory to the recovery list.</li> </ul>
Recovering DISASTER_RECOVERY:\ save set	You must use the <code>recover</code> command in non-interactive mode.
Recovering NDMP data	When restoring NDMP data, relocate the data to a directory that differs from the original location. The NDMP protocol does not support name conflict resolutions. NetWorker overwrites existing files that have the same name as the recovered file. To relocate the data, run the <code>recover</code> command and then type: <code>relocate destination_directory_name</code> . <a href="#">Performing NDMP recoveries on page 586</a> provides details about NDMP recoveries.
Performing directed recoveries	You must use the <code>recover</code> command in interactive mode. You cannot perform a save set restore. <a href="#">Directed recoveries on page 348</a> provides detailed information about a directed recovery.
Performing save set recoveries	Use user accounts with root (UNIX) or Administrator (Windows) permissions. You cannot perform a directed save set recover. Perform concurrent recoveries from an advanced file type by either using multiple <code>-S</code> options to identify multiple save sets, or starting multiple <code>recover</code> commands.

To recover data by using the `recover` command, use the following syntax:

```
recover -a -s NetWorker_servername -c source_host -S ssid/cloneid -d
destination_directory -R destination_host -i recover_option
[directory_name]
```

where:

- `-a` is used to perform the recovery in non-interactive mode. You cannot use the `-a` option with the `-R` option. You cannot use the `-a` option to restore the `DISASTER_RECOVERY:\` save set.
- `-s NetWorker_servername` specifies the name of the source client's NetWorker server. When you do not specify `-s`, `recover` attempts to connect to the first host specified in the `servers` file. The `servers` file, located in `/nsr/res`, contains an entry for each available server.
- `-c source_host` specifies the source host. When you do not specify `-c`, NetWorker assumes that the source client is the host where you run the `recover` program.

- `-S ssid/cloneid` used to perform a save set recover. The `ssid/cloneid` specifies the save set to recover. To recover a clone save set, specify the ssid and cloneid. You cannot use the `-S` option with the `-R` option.
- `-d destination_directory` specifies the full path to the directory on the destination client for the recovered files. Ensure that you use proper syntax for platform of the destination client.
- `-R destination_host` specifies the destination host to receive the recovered data. When you do not use the `-R` option, the host where you run the recover program is the destination host. You cannot use the `-R` option with the `-S` option or the `-a` option. Requires the use of the `-i recover_option` option.
- `-i recover_option` specifies how NetWorker handles a naming conflict between a recovered file and an existing file. Required when you use the `-R` option.  
For example:
  - `iN` does not recover the file when a conflict occurs.
  - `iY` overwrites the existing file when a conflict occurs.
  - `iR` renames the file when a conflict occurs. The recover process appends a `.R` to each recovered file name.
- `source_directory` specifies the initial directory in which to begin browsing.

The *EMC NetWorker Command Reference Guide* or the UNIX man pages provide more information about the recover command and available options.

Example: Performing a recover in interactive mode

1. Type: `recover`
2. To select the files or directories to recover:
  - a. Specify the directory to browse, for example:

```
recover> cd /var/adm
```

- b. Select the file or directory for recovery:

```
recover> add file_name
```

3. To view the selected files or directory:

```
recover> list
```

4. To view the list of the volumes that NetWorker requires to recover the data:

```
recover> volumes
```

5. To recover the files to a location that differs from the original location, type:

```
recover> relocate path
```

6. To start the recovery operation, type:

```
recover> recover
```

7. When the recovery process completes, messages similar to the following appear:

```
Received 1 file(s) from NSR server `jupiter'
Recover completion time: Tue Jan 21 08:33:04 2009
recover>
```

8. To close the `recover` program, type `Quit`.

Example: Performing a recover in non-interactive mode:

To recover a directory `/testdir` on client mars to a new directory `/newdir` on client mars, type:

```
recover -d /newdir -a /testdir
```

Example: Save set recover from command line

To recover a directory `/testdir` from a save set with a ssid of 12345678 and overwrite any existing files with the same name, type this command:

```
recover -S 12345678 -iY /testdir
```

Example: Performing a directed recover

To recover a directory `c:\mydir` that was backed up on client mars to client jupiter, type:

1. On client mars, type:

```
recover -R jupiter -iY
```

2. Add the `c:\mydir` directory:

```
recover> add c:\mydir
```

3. Recover the files:

```
recover> recover
```

## Using the NetWorker User program

Use the NetWorker User program to recover file system data when the administering client is Windows. To recover application data for Microsoft applications that are protected with NMM (NetWorker Module for Microsoft Applications) use the NetWorker Module for Microsoft Applications Client User program. The *EMC NetWorker Module for Microsoft Applications Administration Guide* provides more information.

### Performing a browsable recover by using NetWorker User

Perform these steps in the NetWorker User program on the administering host.

#### Procedure

1. Select the NetWorker server when prompted.
2. From the **Operations** menu, select **Recover/Directed**. To perform a save set recover, select **Save Set Recover**.
3. Select the source host that has the data you want to recover, then click **OK**.
4. Select the destination host for the recovered data, then click **OK**.
5. Mark the files and directories to recover, in the **Recover** window.

---

#### Note

When a drive letter is not present on the destination client, the drive appears with a red question mark.

6. Select optional recover options. The following table summarizes the available recovery options.

**Table 53** Optional browsable recovery options

Recover option	Details
Change the browse time	<p>The <b>Recovery</b> window appears with the latest version of the backup files. To change the browse date and time for all files in the Recovery window:</p> <p>Select <b>View &gt; Change Browse Time</b></p> <p>On the <b>Change Browse Time</b> window, select a new day within the calendar. Select <b>Previous Month</b> or <b>Next Month</b> to change from the current month.</p> <p>In the <b>Time</b> field, change the time of day by typing an hour, minute, and the letter a (for a.m.) or p (for p.m.). Use the 12-hour format.</p> <p>Click <b>OK</b>.</p>
View all versions of a selected file or directory	<p>The <b>Recovery</b> window appears with the latest version of the backup files. When you mark a file system object for example, a file or directory, you recover the last backup version. To view earlier versions of file system objects:</p> <p>Highlight the file or directory that you want to review.</p> <p>Select <b>View &gt; Versions</b>.</p> <p>Select a previous version.</p> <p>Select <b>Change Browse Time</b>.</p> <p>When prompted to change the browse time, click <b>OK</b>.</p> <p>Mark the new version of the file system object.</p>
Search for file system objects	<p>To search for file system objects in the defined browser time:</p> <p>From the <b>File</b> menu, select <b>Find</b>.</p> <p>Type the name of the file or directory. Use wildcards to expand the search; without wildcards, partial file names result in no match being found.</p>
Relocate the recovered file system objects	<p>By default, NetWorker recovers file system objects to their original location. To relocate the files to a different location:</p> <p>Select <b>Options &gt; Recover Options</b></p> <p>In the <b>Relocate Recovered Data To</b> field, type the path on the destination host to recover the data, then click <b>OK</b>.</p> <p>For NDMP data restores, the target path is a literal string and must match the path as seen by the NAS filer in its native OS. Otherwise, NetWorker recovers the files to the original location and overwrites the existing file host with the same name. <a href="#">Performing NDMP recoveries on page 586</a> provides details about NDMP recoveries.</p>
View volumes required for recovery	<p>Before you start the recovery operation, monitor which volumes NetWorker requires to recover the selected file system objects.</p> <p>To view the required volumes, select <b>View &gt; Required Volumes</b>.</p> <p>Ensure the listed volumes are available or NetWorker to mount into an available device.</p>
Resolve name conflicts	<p>By default, the Naming Conflict window appears each time there is a file name conflict during a recovery. To specify the method to automatically resolve all name conflicts:</p> <p>Select <b>Options &gt; Recover Options</b>.</p>

**Table 53** Optional browsable recovery options (continued)

Recover option	Details
	<p>Select a conflict resolution option:</p> <ul style="list-style-type: none"> <li>• Rename the recovered files. By default, the recover operation appends a tilde (~) to the beginning of the name of the recovered file <code>~file name</code>. When a file named <code>~file name</code> already exists, the recovered file is renamed <code>~00_file name</code>, and so forth to <code>~99_file name</code>. When this fails, the recover process does not automatically rename the file and prompts the user to specify a name for the file.</li> <li>• Discard recovered file: Discards the recovered file and keeps the existing file.</li> <li>• Overwrite existing file: Replaces the file on the file system with the recovered version.</li> <li>• Overwrite and replace a reboot: Replaces the file on the file system with the recovered version after you reboot the destination host. NDMP recoveries do not support resolving name conflicts NDMP recoveries always overwrite existing files. Relocate the NDMP data to a different location to avoid data loss. <a href="#">Performing NDMP recoveries on page 586</a> describes how to perform NDMP recoveries</li> </ul>

7. Click **Start** to begin the recovery. It takes the NetWorker server a few moments to recover the files, depending on file size, network traffic, server load, and tape positioning. During this time, messages appear so that you can monitor the progress of the recovery.

When the recovery is successful, a message similar to this appears:

```
Received 1 file(S) from NSR server server
Recover completion time: Tue Jan 21 08:33:04 2009
```

#### NOTICE

When an error occurs while recovering Microsoft Exchange Server or Microsoft SQL Server data by using VSS, you must restart the recovery process. When the recovery fails due to a problem with VSS or a writer, an error message appears. Use the Windows Event Viewer to examine the event logs for additional information. VSS recovery error messages are also written to the NetWorker log file.

## Performing a save set recover by using NetWorker User

Use the NetWorker User program to perform a save set recover when the administering host is a Windows system.

#### NOTICE

Only members of the Windows Administrators group have permission to perform a save set recovery.

Perform these steps in the NetWorker User program, on the administering host.

### Procedure

1. Select the NetWorker server when prompted.

2. Select **Operation > Save Set Recover**.
3. Select the source host that has the data you want to recover, then click **OK**.
4. In the **Save Sets** window, select the name of the save set from the **Save Set Name** list.
5. Select the version of the save set (if there are multiple versions). When required, select the cloned version of a save set if one is listed.
6. Select optional recover options. The following table summarizes the recover options available with a save set recovery.

**Table 54** Optional save set recovery options

Recover option	Description
Specify file system objects	<p>By default, NetWorker recovers all selected files and directories. To recover only certain file system objects in a save set:</p> <p><b>Click Files...</b> Specify the files and directories to recover, one full path per line. <b>Click OK.</b></p>
View required volumes	<p>Before you start the recovery operation, monitor which volumes NetWorker requires to recover the selected file system objects. <b>To view the required volumes, select Required Volumes.</b> Ensure the listed volumes are available for NetWorker to mount into an available device.</p>
Relocate the recovered file system objects	<p>By default, NetWorker recovers file system objects to their original location. To relocate the files to a different location:<b>Select Recover Options.</b> In the <b>Relocate Recovered Data To</b> field, type the full path of the directory where the data should be relocated and then click <b>OK</b>. For NDMP data restores, the target path is a literal string and must match the path as seen by the NAS filer in its native OS. Otherwise, the recover process uses the original location and overwrites existing files with the same name. <a href="#">Performing NDMP recoveries on page 586</a> provides details about NDMP recoveries.</p>
Resolve name conflicts	<p>By default, the Naming Conflict window appears each time there is a file name conflict during a recovery. To specify the method to automatically resolve all name conflicts:</p> <p><b>Select Options &gt; Recover Options.</b></p> <p>Select a conflict resolution option:</p> <ul style="list-style-type: none"> <li>• Rename the recovered files. By default, a tilde (~) is appended to the beginning of the name of the recovered file <i>~file name</i>. When a file named <i>~file name</i> already exists, the recovered file is renamed <i>~00_file name</i>, and so forth to <i>~99_file name</i>. When this fails, the recover process does not automatically rename the file and prompts the user to specify a name for the file.</li> <li>• Discard recovered file: Discards the recovered file and keeps the existing file.</li> <li>• Overwrite existing file: Replaces the file on the file system with the recovered version.</li> <li>• Overwrite and replace a reboot: Replaces the file on the file system with the recovered version after you reboot the destination host. NDMP recoveries do not support resolving name conflicts. NDMP recoveries always overwrite existing files. Relocate the NDMP data to a different location</li> </ul>

**Table 54** Optional save set recovery options (continued)

Recover option	Description
	to avoid data loss. <a href="#">Performing NDMP recoveries on page 586</a> describes how to perform NDMP recoveries

- Click **OK** to begin the recovery. It takes the NetWorker server a few moments to recover the files, depending on file size, network traffic, server load, and tape positioning. During this time, messages appear so that you can monitor the progress of the recovery.

When the recovery is successful, a message similar to the following appears:

```
Received 1 file(S) from NSR server server
Recover completion time: Tue Jan 21 08:33:04 2009
```

## Using the scanner program to recover data

You can use the `scanner` program to recover data from a volume by save set ID (`ssid`) to the host that starts the program. Ensure that the operating system of the NetWorker host that runs the `scanner` command is the same operating system of the source client.

### NOTICE

You cannot use the `scanner` command recover data from a NetWorker Module, NDMP or DSA save set.

### Procedure

- Ensure the value in the **Idle device timeout** attribute of the device that contains the volume is 0. [Unmounting volumes automatically \(idle device timeout\) on page 217](#) provides more information.
- Use the `mminfo` program to query the media database for save set information.

For example:

```
mminfo -avq ssid=ssid -r volume,client,name,ssid,mediafile,mediarec
```

where `ssid` is the save set ID associated with the data.

- Use the save set information from the `mminfo` command to run the `scanner` program:
  - To recover all files in a save set on Windows, type:

```
scanner -v -S ssid -f mediafile -r mediarec device | path\uasm -rv
```

where:

- `ssid` specifies the save set ID value obtained from the `mminfo` output.
- `mediafile` specifies the starting file number of the save set, obtained from the `mminfo` output.
- `mediarec` specifies the starting file record number of the save set, obtained from the `mminfo` output.

- *device* is the name of the device that contains the volume. *is* the name of the device the volume is loaded in, for example `/dev/rmt0.1` or `\.\Tape0`
- *path* is the path on the NetWorker host that contains the uasm binary. For example, on Windows:  
`C:\Program Files\EMC NetWorker\bin`

## Scanner command examples

### Recovering a single file to a different location on Windows

To recover a single file in the save set on Windows to a different location, type:

```
scanner -v -S ssid -f mediafile -r mediarec device | path\uasm -rv -m
source_dir=dest_dir filename
```

where:

- *source\_dir* is the directory where the data resided during the backup.
- *dest\_dir* is the directory where the data is relocated during the recovery.
- *filename* is the name of the file or directory to recover.

### Recover a complete save set on UNIX

To recover all files in a save set on UNIX, type:

```
scanner -v -S ssid -f mediafile -r mediarec device -x path/uasm -rv
```

### Recovering a single file to a different location on UNIX

To recover a single file in the save set on UNIX and to a different location, type:

```
scanner -v -S ssid -f mediafile device -x path/uasm -rv -m
source_dir=dest_dir filename
```

The *EMC NetWorker Command Reference Guide* or the UNIX man pages provide more information about the `scanner` program.

## Using VSS file level recovery (FLR)

Currently, the system state files are filtered out using VSS directives created when VSS is initialized and processed. Not applying the VSS directives adds the system state back into the volume backups. The directives for exclude file list and un-supported writers (application writers) generated from VSS are applied.

For any volume backup used in online incremental system state or offline incremental disaster recovery, every file system backup must be VSS consistent. In order to create VSS consistent backups, system state writers that are affected by this backup must participate in the file system backup, even if the backup includes a single file. For example, when backing up `C:\dir1\file1`, the VSS writers which protect files on `C:\` must participate in the snapshot, but only a snapshot of `C:\` is created.

This behavior may not be appropriate for certain circumstances. Use the command line flag `VSS:=off`, to remove this VSS requirement. However, to create a valid backup of any system critical volume, the Windows VSS mechanism must be used.

For incremental backups of any level other than full, time of the last change is used to determine whether a file needs to be included or not. This is not an issue for most system state files. For certain database files such as SQL files used by WID writer, the time of the last change may not reflect the latest updates to the file.

A new option, replace at reboot, is available during the recovery procedure. When this option is selected, file conflicts replace the target file with the contents of the source file.

If any of the files are in use, they are replaced at reboot. This option is disabled if the target computer is different from that of the source.

This functionality is available for both browse based restore and BBB backup restores.

File Level Recovery is available from any supported web browser. You select a date and time of a backup to mount, and then select the option for specific files from the selected backup. You may restore a file to the original destination, or to a new destination on the VM. You can also restore files from a backup to a New VM.

VSS FLR restore of system state files using directed recovery renders the target host unstable. Restoring system state data, for example, registry C:\system32\config, or side by side files to another system, for example, C:\windows\winsxs, via directed recovery leaves the target host unstable or not bootable.

## Recovering deduplication data

The *EMC NetWorker Avamar Integration Guide* and the *EMC NetWorker Data Domain Deduplication Devices Integration Guide* provides more information on how to recover deduplication data.

## Recovering with BMR

[Windows Bare Metal Recovery on page 611](#) provides information on performing a Windows BMR recovery with NetWorker.

## Recovering ACL files

NetWorker now provides the ability to browse and recover files with associated ACLs (Access Control Lists) in directories for which the user is not the primary owner.

To recover files with associated ACLs, ACL passthrough must be checked in the Recover section of the NetWorker Server Properties window. The feature is enabled by default.

If ACL passthrough is disabled, the following message is displayed when a non-owner attempts to browse ACL files in the directory:

```
Permission denied (has acl)
```

---

### Note

ACLs and extended attributes for files are not recovered when files are recovered to a different operating system file system as can be the case in a directed recovery.

## Recovering encrypted data

To recover data that was encrypted with the current AES pass phrase, no special action is required. However, to recover data that was encrypted with an AES pass phrase that is different than the current pass phrase, follow the procedure in this section.

The current pass phrase is listed in the Datazone Pass Phrase attribute of the NetWorker server. [Setting the Datazone pass phrase for a NetWorker server on page 103](#) provides more information.

To recover AES encrypted data that was not encrypted with the current pass phrase:

- Use the `-p` option with the command that is being used to recover data. For example:

```
recover -p pass_phrase
winworkr -p pass_phrase
```

To enter multiple pass phrases with the `-p` option, type:

```
recover -p pass_phrase1 -p pass_phrase2 -p pass_phrase3
```

- Specify the pass phrase(s) in the **Pass phrase** field in the NMC Recovery Wizard.

**NOTICE**

When an incorrect pass phrase or no pass phrase is entered, encrypted data is not recovered. Instead, the file names are created without data. However, if unencrypted data is also selected for recovery, it is recovered.

---

## Recovering Windows volume mount points

A volume mount point (or mount point) is a disk volume that is grafted into the namespace of a host disk volume. This allows multiple disk volumes to be linked into a single directory tree, similar to the way DFS links network shares into a unified structure.

Assigning a drive letter to a mount point is optional. Many disk volumes can be linked into a single directory tree, with a single drive letter assigned to the root of the host volume.

### Recovering mount points

Perform separate recovery operations to recover the mount point and the mounted volume's data.

**NOTICE**

The NetWorker Save Set Recovery feature does not support recovery of mount points. To recover mount points and their data, use these special procedures. Recovering a mount point and its data

---

#### Procedure

- Manually create the mountpoint, if it does not exist already.
- Start the NetWorker User program and recover the data under the mount point.

#### Results

[Using the NetWorker User program on page 361](#) provides more information about performing data recoveries.

### Recovering nested mount points

#### Procedure

- When the mount points do not already exist, manually create the top-level mount point, then work down the hierarchy and create each successive mount point.
- Start the NetWorker User program and recover the data under the mount points.

# Recovering special Windows databases

This section describes how to recover Windows system databases:

- [Recovering Windows DHCP and WINS databases on page 369](#)
- [Recovering expired save sets on page 369](#)

## Recovering Windows DHCP and WINS databases

Use the following procedures to perform an offline recovery of the DHCP and WINS databases.

**NOTICE**

When you recover from a save set ALL backup, the recovery operation automatically recovers the DHCP and WINS, and these procedures are not required.

### Recover a DHCP database

**Procedure**

1. Use the NetWorker User program to recover the %SystemRoot%\System32\dhcp directory.
2. Use the Microsoft DHCP administrative tools to restore the DHCP database. The Microsoft documentation provides detailed instructions about Microsoft DHCP administrative tools.

### Recovering a WINS database

**NOTICE**

Microsoft documentation describes how to use the Microsoft WINS administrative tools to recover the databases.

**Procedure**

1. Use the NetWorker User program to recover the backup configured in the WINS backup procedure. [Backing up Windows DHCP and WINS databases on page 109](#) provides more information.
2. Use Microsoft WINS administrative tools to restore the WINS database.

## Recovering expired save sets

Each NetWorker client, including the NetWorker server has a client file index. This database contains information about the files that are in a save set. When a save set browse policy expires, it is no longer available for recovery by file selection, that is, it is no longer browsable for recovery. Some applications such as the NetWorker Module for Databases and Applications programs require that the save set is browsable to perform the recovery.

You can make expired save set files browsable for recovery by adding the save set information back into the client file index. The procedure to recover the save set entry into the client file index depends on the state of the save set in the media database.

## Recovering a recyclable or recoverable save set entry in the online indexes

This section describes how to recover save set information into the client file index when the save set is the media database and save set status is recyclable or recoverable.

The ssflags attribute identifies the status of a save set. The `mminfo` command displays the ssflags attribute:

- A save set is recoverable when ssflags contains a r. This save set has exceeded its defined browse policy.
- A save set is eligible for recycling when ssflags contain an E. This save set has exceeded its defined retention policy. This is also referred to as an expired save set.

The *EMC NetWorker Command Reference Guide* describes how to use the `mminfo` command.

[Recovering a save set entry into the client file index and media database on page 374](#) describes how to add save sets to the media database and client file index if they no longer exist.

### Using `mminfo` to generate save set information

Gather the save set information.

#### Procedure

1. Login to the NetWorker server as root or the Windows administrator account.
2. Query the media database on the NetWorker server for the NetWorker client that requires modification:

```
mminfo -avot -c client_name
```

where *client\_name* is the name of the recovery client.

3. Record the following values for the save sets to add into the client file index:

- ssid column
- date of the backup
- lvl column. When the lvl value is anything other than full, ensure that you record the ssid and dates for the previous full backup and all level backups in between.

For example:

```
<NetWorker_install_path>\nsr\bin>mminfo -avot -c swift
Volume           client   date      time
size    ssid      fl  lvl     name
snapimagewin1.001  swift    11/5/2009  12:02:18 PM   83
KB      4294078835   CE    full    c:\bkup
snapimagewin1.001  swift    11/5/2009  12:02:23 PM   4
KB      4277301623   cr    full    index:swift
snapimagewin1.001  swift    11/5/2009  12:02:25 PM  141
KB      4260524409   cr    full    bootstrap
```

In this procedure, and all of the following examples, the ssid 4294078835 is used for the client swift11.

4. Obtain the cloneid for the recorded save sets:

```
mminfo -q ssid=ssid_number -r cloneid
```

where *ssid\_number* is the ssid number provided in the previous `mminfo` command.

For example:

```
mminfo -q ssid=4294078835 -r cloneid
1257402739
```

When more than one ssid was recorded, repeat this step for all ssids.

## Using nsrmm to modify the save set properties

Modify the save set properties.

### Procedure

1. When the save set is recyclable:

a. Modify the save set entry to make it recoverable with the *nsrmm* command:

```
nsrmm -e MM/DD/YYYY > -S ssid/cloneid
```

where:

- *MM/DD/YYYY* is the date chosen to make the save set browsable from.
- *ssid/cloneid* is the save set id/cloneid.

For example:

```
nsrmm -e "11/21/2009" -S 4294078835/1257402739
```

When more than one ssid was recorded, repeat this step for all ssids.

b. Modify the save set to the **not recyclable** status:

```
nsrmm -o notrecyclable -S ssid/cloneid -y
```

where *ssid/cloneid* is the save set id/cloneid.

For example:

```
nsrmm -o notrecyclable -S 4294078835/1257402739 -y
```

When more than one ssid was recorded, repeat this step for all ssids.

c. Verify that the save set status is recoverable:

```
mminfo -q ssid=ssid -r sumflags
```

Recoverable save sets have an r, in addition to other values in the sumflags output.

For example:

```
mminfo -q ssid=4294078835 -r sumflags cr
```

When more than one ssid was recorded, repeat this step for all ssids.

2. Query the media database to confirm that the index save set for a client is recoverable:

```
mminfo -avot -N index: client_name
```

where *client\_name* is the name of the client to which this save set is located.

3. Confirm that the value in the *f1* column is *cr* for an index backup with the time frame of the client save set to be restored.

**NOTICE**

When the index save set is not recoverable, the save set will expire when the NetWorker software cross checks the indexes. For example `nsrim -X`.

4. Record the values in the date and time columns.

## Rep populating the client file index

Use the `nsrck` or `scanner` command to repopulate the client file index with information about files in a save set.

### **Repopulate the client file index by using the `scanner` program**

Use the `scanner` program to repopulate the client file index with information about files and directories for a specific save set.

The entries assume the browse policy of the original save set. For example, suppose a save set originally had a browse time of one month and a retention time of three months. However, the browse and retention times have expired. When you restore the save set entry by using the `scanner` program, the save set then remains browsable for one month and recoverable for three months.

To Repopulate the client file index by using the `scanner` program, perform the following steps:

#### **Procedure**

1. Ensure the **idle device timeout** value of the device containing the volume is 0. Refer to [Unmounting volumes automatically \(idle device timeout\) on page 217](#) for details.
2. Query the media database using the `mminfo` program for save set information:

For example:

```
mminfo -avq ssid=ssid -r volume,client,name,ssid,mediafile,mediarec
```

where `ssid` is the associated save set id for the data you want to recover.

3. Use the information from the `mminfo` command for the save set to run the `scanner` program. When the save set spans more than one volume, scan the volumes in the order in which they were written:

```
scanner -v -i -S ssid -f mediafile -r mediarec device
```

where:

- `mediafile` is the starting file number for the save set, obtained from the `mminfo` output.
  - `mediarec` is the starting record number for the save set, obtained from the `mminfo` output.
  - `device` is the name of the device the volume is loaded in, for example `/dev/rmt0.1` or `\.\Tape0`.
4. When the save set spans multiple volumes, the `scanner` program prompts for a new volume as needed.

**NOTICE**

The `-i` option is not supported for cloud devices.

## Rep populating the client file index by using the nsrck program

Use the `nsrck` program to repopulate the client file index with information about all save sets for the client up to the date and time specified.

### Procedure

1. Ensure that the volume containing the index backup is available.
2. Use the `nsrck` command to repopulate the client file index:

```
nsrck -L 7 -t MM/DD/YYYY client_name
```

where:

- where *client\_name* is the name of the client with the data to be recovered.
- *MM/DD/YYYY* is the backup date of the save set.

For example:

```
<NetWorker_install_path>\nsr\bin>nsrck -L 7 -t "11/21/2009" swift
nsrck: checking index for 'swift'
9343:nsrck: The file index for client 'swift' will be
recovered.Requesting 1 rec
over session(s) from server
Recover completion time: 11/20/2009 1:45:55 PM
nsrck: <NetWorker_install_path>\nsr\index\swift contains 12
records occupying 2 KB
nsrck: Completed checking 1 client(s)
```

When you recover a client file index from a time and date in the past, `nsrck` adds the full contents of the index from that time and date to a temporary subdirectory of the client file index directory. When a time value is not specified, everything for the specified date (up to 23:59) is included. After the index has been read from the backup media, the required index data is integrated fully into the client file indexes and the temporary subdirectory is removed. The “required index data” includes the indexes from the date specified to the first full backup that occurred prior to the date specified.

Be aware that if a saveset from the specified date runs into the next day, which would be Nov 22, 2009 in this example, then the index required to browse the saveset will not be recovered. To recover this index, you would have to specify Nov 22, 2009 as the recovery date as shown in the following command:

```
nsrck -t "11/22/2009" -L7 swift
```

A check on the required index date may be necessary if index backups are set to be taken once daily. When the back up of the index does not take place until the following day, the date of the following day must be specified.

3. Confirm that the client save sets are now browsable:

```
mminfo -q ssid=ssid -r sumflags
```

Browsable save sets contain a b, in addition to other values in the sumflags output.

For example:

```
NetWorker_install_path\nsr\bin>mminfo -q ssid=4294078835 -r
sumflags
cb
```

4. Perform a file-by-file recovery by using the NetWorker User program (Windows), the **recover** command or the NMC Recovery Wizard.

## Recovering a save set entry into the client file index and media database

When a volume contains a save set that does not appear in the media database, the **scanner** command is used to restore save set information into the media database and optionally, the client file index.

To rebuild the save set's entry in the media database and the client file index, perform the following steps.

### Procedure

1. Log in as root or a Windows Administrator.
  2. At the command prompt, run the **scanner** program on the volumes that contain the appropriate file or files:
- ```
scanner device_name
```
3. Use the output from the **scanner** program to determine:
    - If the volume contains the save set that you want to scan.
    - If you want to scan the contents of the volume in the online indexes.
    - If the save set spans multiple volumes.
  4. Load the first volume containing the save set information into an available device. Ensure the **Idle Device Timeout** value for the device is 0. Refer to [Unmounting volumes automatically \(idle device timeout\)](#) on page 217 for details.
  5. Use the **scanner** command to repopulate the NetWorker databases:
    - To repopulate the media database with the save set information, type the following command:

```
scanner -m -S ssid device_name
```

- To repopulate the media database and client file index with the save set information, type the following command:

```
scanner -i -S ssid device_name
```

#### NOTICE

When the volume contains data from an earlier version of NetWorker, there may be no pool information on the volume. In this case, the volume is considered to belong to the Default pool. To assign the volume to another pool, use the **-b pool\_name** option in this step. When the volume already belongs to a pool, the **-b** option will have no effect.

6. Recover the data.

## Recovering client files on a different NetWorker server

You can use a NetWorker server, which differs from the original NetWorker server to recover data for a client.

### Before you begin

Determine the pool names that were used to write the client data to the media on the original NetWorker server.

To use a different NetWorker server to recover client data, you must perform the following tasks on the new NetWorker server:

- Create a client resource with the same client ID that the original NetWorker server associated with the client name.
- Create each pool resource that was used to write the client data to a volume.
- Use the `scanner` command to repopulate the media database and client file indexes with save set information for the client.

### Procedure

1. Determine the **Client ID** value of the NetWorker client on the original server:
  - a. On the **Administration** window, click **Configuration**.
  - b. In the left pane, click **Clients**.
  - c. In the right pane, right-click the client, and then select **Properties**.
  - d. On the **Globals (1 of 2)** tab, make note of the value in **Client ID** attribute, then click **Cancel** to close the **Properties** window.
2. On the new NetWorker server, create a new client:
  - a. In the **Name** attribute, type a name for the client.
 

You can use the same name that was used on the original server, but you cannot use a name that exists on the new server. When a client with the same name exists on the new server, use this format to specify the client name:

`~hostname-#`

where *hostname* is the hostname of the client.

For example, if the client's hostname is *jupiter*, and a client named *jupiter* already exists on the new server, type:

`~jupiter-1`
3. On the new NetWorker server, create each pool resource that was used to write the client data on the original NetWorker server.

#### Note

Ensure that you create each pool resource with the same name that you used on the original NetWorker server.

4. Use the `scanner` command to import the save set information into the new NetWorker server.
  - To import the save set information into the client file index and media database entries, type the following command:
 

```
scanner -i -c client_name device_name
```

 where *client\_name* is the name of the client that appears on the original NetWorker server.
  - To import the save set information into the media database only, type the following command:
 

```
scanner -m -c client_name device_name
```

 where *client\_name* is the name of the client that appears on the original NetWorker server.

**NOTICE**

When you use the `scanner -i` or `scanner -m` to import data before you configure the Client resource on the new server:

- Only the media database will contain the client ID and save set information for the imported save sets.
  - If the same hostname already exists on the NetWorker server, NetWorker will not use the original hostname to store the save set information because the client ID is different. NetWorker will associate the save set information with a hostname in the format `clientname-#`.
  - You must create a new client resource with the name `clientname-#` and specify the client ID that you recorded from the original NetWorker server.
  - Optionally, after you create the new client resource, run the `scanner -i` command to store the save set information into the client file index. When you use the `scanner` command, specify the client name as it appears on the original NetWorker server.
- 

## Recovering critical NetWorker server databases

Protecting a NetWorker server including its critical databases requires careful planning and preparation. The recovery methods described in this section may not work if the NetWorker server is not adequately protected. Information about protecting a NetWorker server is provided in the *EMC NetWorker Server Disaster Recovery and Availability Best Practices Guide*.

The databases that are critical to the recovery of a NetWorker server include the bootstrap and the client file indexes.

A bootstrap includes the:

- Media database, which contains the volume location of each save set.
- Resource files which contains all of the resources, such as NetWorker clients and backup groups, that are defined on the NetWorker server.

The client file indexes include tracking information for each file that belongs to a client's save sets. There is one client file index for each NetWorker client.

Starting in NetWorker 8.1 there is a command line program named `nsrdr` that simplifies the recovery of the NetWorker server's media database, resource files, and client file indexes. Previously, you had to use the `mmrecov` command to recover the media database and resource files, and the `nsrck` command to recover client file indexes. These commands are still available. The *EMC NetWorker Command Reference Guide* and the UNIX man pages contain information about these commands and the `nsrdr` command.

Use the procedures in this section to recover lost or corrupted bootstrap or client file indexes. If your server databases are not corrupted and you only need to restore expired save set entries into the client file index or the media database, you can use the procedures in [Recovering expired save sets on page 369](#). Save sets are removed from the client file index when their browse policy time has expired. Save set entries are removed from the media database when their retention policy time expires.

The `nsrdr` command is flexible. You can run the `nsrdr` program in fully interactive mode and respond to questions or you can run the program silently with command line options. You can recover the media database, resource files, and all client file indexes in

one operation, or recover just one item by itself. If you are recovering client file indexes, you can also recover the indexes for just one or a small number of NetWorker clients instead of recovering all client file indexes for all clients in one operation.

To help troubleshoot issues with the wizard, messages are logged to the following locations:

- On UNIX, /nsr/logs/nsrdr.log
- On Windows, <NetWorker\_install\_path>\nsr\logs\nsrdr.log

## Prerequisites to recover the NetWorker server databases

Depending on the state of your NetWorker server, you may have to do some preparation before you can recover the bootstrap and client file indexes. There are two main scenarios to consider, this guide covers scenario 1 only:

- Scenario 1: lost bootstrap or client file indexes  
In this scenario you just need to recover the NetWorker server bootstrap or client file indexes because they have been lost or deleted. The NetWorker server software and hardware is intact but you notice that some bootstrap data such as the media database or NetWorker server resources are missing or incomplete. Additionally, you may notice that some clients are no longer browsable for recovery even though they have not exceeded their browse retention time policies; this indicates missing or incomplete client file indexes.
- Scenario 2: disaster recovery  
In this scenario, the NetWorker server host has suffered some damage, such as a disk or power supply failure, and the base operating system might have been removed or corrupted. In this scenario, the hardware must be replaced and a fresh install of the software is required. The steps in this section are beyond the scope of a disaster recovery. The NPG (NetWorker Procedure Generator) provides disaster recovery steps. Additionally, you should follow the practices described in the *EMC NetWorker Server Disaster Recovery and Availability Best Practices Guide* to reduce the likelihood of encountering a disaster recovery scenario and to maximize the likelihood of successfully recovering from a disaster.  
The NPG and all user documentation can be downloaded from EMC Online support. To access the NPG, log on to <https://support.emc.com/> and search for NetWorker Procedure Generator. You must have a service agreement to use this site.

Before recovering lost bootstrap or client file indexes, ensure that the following prerequisites are met.

### Is the NetWorker server is installed?

If you need to reinstall the NetWorker server software, refer to the disaster recovery steps in the NPG (NetWorker Procedure Generator). These procedures are located in the NPG by selecting the options titled Recovering with NetWorker > Disaster Recoveries > Server.

### Is the bootstrap report available?

Bootstrap report information includes the following:

- Bootstrap SSID (Save Set Identification Number)
- Volume name containing the bootstrap
- File-number and record-number of the tape media (if used) where the bootstrap information starts

To obtain the bootstrap, perform the following steps.

1. Use one of the following methods to obtain the bootstrap:

- Save Group Completion Report. [Bootstrap report generation on page 254](#) describes how to send the Save Group Completion report to an email address on a regular basis.
- Locate the bootstrap SSID and volume name in the messages log file.
  - On UNIX, /nsr/logs/messages
  - On Windows, <NetWorker\_install\_path>\nsr\logs\messages
- If the media database is not lost and the volume list is available then obtain bootstrap information by running this command:
 

```
mminfo -av -B -s server_name
```
- Let the nsrdr command scan the device for the bootstrap information. For existing devices, nsrdr will detect the latest bootstrap on a volume that contains the bootstrap information.
 

If the bootstrap is on a disk volume such as an AFTD volume, and you need to create the corresponding AFTD device to access the volume, special precautions are required to prevent the inadvertent destruction of the bootstrap data. Follow the considerations in [Is a local device available? on page 378](#) to ensure that you do not destroy the bootstrap data on the volume when adding the device.

If the bootstrap is on a cloud device and you need to re-create it, refer to the considerations in [Is the bootstrap on a cloud device? on page 378](#).
- If you cannot locate the bootstrap volume using any of the previous methods, refer to the disaster recovery procedures in the EMC NetWorker SolVe Desktop (formerly known as the NetWorker Procedure Generator).

## Is a local device available?

The NetWorker server requires a local device resource to back up the bootstrap data. You can use the same device resource to recover the bootstrap data. In the unlikely case where you need to add a local device because the original device resource is lost, keep the following considerations in mind:

- Do not relabel the volume when you create the device. Relabeling a volume with bootstrap backups, or any other backups, will render the data unrecoverable.
- Additional requirements for disk based devices such as AFTD.
  - Do not allow the device wizard to label the disk volume. The **Label and Mount** option on the wizard's Device Label and Mount window has this option selected by default. Uncheck the **Label and Mount** option.
  - Specify the local path to the AFTD volume in the device wizard Select Storage Node window. Ensure that this is the same path on which the bootstrap data is stored.

## Is the bootstrap on a cloud device?

If the bootstrap is on a cloud device, review the following information.

- If the bootstrap is on a cloud device and the cloud device resource has been lost, re-create a cloud device resource. [Cloud devices on page 173](#) provides more information.
- Determine the name of the volume that contains the bootstrap. If the original server is not available or the bootstrap report is lost and you do not know the cloud volume name, you can obtain it by checking the Atmos server. The volume name can be

- found in the following location on the Atmos server: /networker/datazone-id/volumes/volume\_name
- Determine the datazone ID of the NetWorker server that was used for the bootstrap backup. If the original server is not available, the datazone ID can be located on the Atmos server in the following location: /networker/datazone-id/volumes/volume\_name  
To locate the datazone ID of the NetWorker server if it is not available:
    - From the NetWorker Server **Administration** window, select **View > Diagnostic Mode**.
    - Right-click the NetWorker server name in the left pane and select **Properties**.
    - In the **System Summary** tab of the NetWorker Server Properties dialog box, record the value in the Datazone id field.

## Consider your recovery options

The `nsrdr` command is flexible and can be run in a variety of ways. However, the major options to consider before running the `nsrd` command are outlined in this section. For a complete list of advanced options, refer to [Options for running the nsrdr command on page 384](#).

### Do you need to recover all client file indexes?

Recovering all client file indexes can take a long time. If you only need to recover the client file indexes for a limited set of clients, use the `nsrdr -I` option, for example:

```
nsrdr -c -I clientA clientB clientD
```

[Options for running the nsrdr command on page 384](#) provides more options for recovering specific client file indexes with the `nsrdr` command.

### Were save sets backed up after the last bootstrap backup?

If save sets were backed up after the last bootstrap backup, then these backup records might be overwritten after the bootstrap is recovered. This situation can only occur when a manual backup is taken. A manual backup does not trigger a bootstrap backup immediately, therefore the manual backup will not be recorded in the bootstrap until the next scheduled backup. To protect against losing save sets that were backed up after the last bootstrap backup, use the `nsrdr -N` or `-N -F` options, for example:

If using a tape volume:

```
nsrdr -N
```

If using a disk based device such as an AFTD:

```
nsrdr -N -F
```

If you know that manual backups were not taken after the last bootstrap backup or you are not concerned about losing these backups, do not use the `-N` or `-N -F` options. These options can increase the time and complexity of the recovery considerably.

## Recovering the NetWorker server databases

The steps in this section assume that you are running the NetWorker server disaster recovery command, `nsrdr`, in fully interactive mode. This is the recommended mode to use in a typical NetWorker server recovery operation. You can also run the wizard with

various command line options depending on what you need to accomplish. [Options for running the nsrdr command on page 384](#) provides more information.

#### Note

Steps one and two are required only if using the -N option with the nsrdr command in step three. [Were save sets backed up after the last bootstrap backup? on page 379](#) provides more information.

#### Procedure

1. Unmount all volumes including tape, file type, advanced file type devices, and cloud volumes.
  - a. In the NetWorker Administration interface, click **Devices**.
  - b. Select **Devices** in the navigation tree. The Devices detail table appears.
  - c. Right-click a device and select **Unmount**.
2. Enable the CDI (Common Device Interface) attribute on all tape devices.

#### Note

NDMP, AlphaStor, and optical devices do not support CDI.

- a. In the NetWorker Administration interface, click **Devices**.
  - b. From the **View** menu, select **Diagnostic Mode**.
  - c. Select **Devices** in the navigation tree. The Devices detail table appears.
  - d. Double-click a device in the Devices table.
  - e. Select the **Advanced** tab. In the Device Configuration area, locate the CDI settings and select **SCSI commands**. The EMC NetWorker Administration Guide provides more details about CDI considerations.
  - f. Stop and restart the NetWorker server services/daemons.
3. Log in as root or Administrator and type one of the following commands at a command prompt:
    - `nsrdr`
    - If your backups are on tape and you want to prevent the possibility of overwriting manual backups that were taken after the last bootstrap backup, type the following command:  
`nsrdr -N`
    - If your backups are on a disk device such as an AFTD (Advanced File Type Device), and you want to prevent the possibility of overwriting manual backups that were taken after the last bootstrap backup, type the following command:  
`nsrdr -N -F`

Using the `-N` or the `-N -F` options set the Scan Needed (scan volflag) flag on ALL appendable (non read-only) volumes that are listed in the recovered bootstrap's media database. When the `-N` option is specified and you attempt to write data to a tape-based device that has newer save sets than what is recorded in the media database, a message displays that explains how to update the media database to avoid the possibility of overwriting the newer data. When the `-N -F` option is used for disk devices such as an AFTD, you can still write to the disk, however, recover space operations will be suspended until the Scan Needed flag is removed. A recover

space operation purges the disk device of any save sets that do not have a corresponding entry in the media database.

If you are sure that no backups were done after the last bootstrap backup or you do not need to recover that data, omit the -N or -N -F options.

4. When asked to continue, type **y** for yes.
5. Select the device that contains the NetWorker server bootstrap save set.
6. Type the save set ID of the latest bootstrap.

If you do not know the save set ID of the latest bootstrap, leave this entry blank and press **Enter**.

- a. Select **Yes** when given the option to scan the device for the latest bootstrap save set ID.

---

#### Note

The option to scan for a bootstrap save set ID is not supported for non-English locales. In this case, use the `scanner` command to find the bootstrap ID.

- b. When the latest bootstrap save set is located, select **Yes** to recover the bootstrap save set.
- c. If you are recovering from tape, you are given the option to input the tape file number and record location number of the bootstrap save set. This information can speed up the bootstrap recovery. Enter this information if you have it.
- d. If you are recovering from a cloud device, you are prompted to enter the name of the cloud volume that contains the bootstrap save set.
- e. If you are recovering from a cloud device, you are prompted to enter the datazone ID of the NetWorker server. Ensure that this is the datazone for the NetWorker server that was used to back up the bootstrap.
- f. Press **Enter**.
- g. If you are recovering from tape, you are prompted to load the volume.

The `scanner` program is run and the bootstrap save set is recovered. The media database is replaced by data from the bootstrap save set. The recovered resource database is saved to a temporary folder named `res.R`. The NetWorker server services are also shut down because the resource database cannot be overwritten while these services are running.

7. Select **Yes** when asked if you want to replace the resource database folder (`res`) with the recovered resource database.

The NetWorker server services are restarted after the resource database folder is replaced with the recovered resource database. The replaced folder is renamed to `res.timestamp`.

8. If you want to recover all client file indexes, select **Yes** when asked if you want to do a client file index recovery. Select **Yes** again when asked to confirm your choice.

You will recover one client file index for each NetWorker client that was backed up including the client file index for the NetWorker server. The wizard ends after the client file indexes are recovered.

If you want to recover the client file index for selected clients only:

- a. Select **No** and exit the wizard.

- b. Re-enter the `nsrdr` command with the `-c -I` options and provide a list of client names with each name separated by a space, for example:

```
nsrdr -c -I clientA clientB clientD
```

The bootstrap recovery is skipped and you are prompted to complete the recovery of the specified client file indexes.

The wizard exits after the client file indexes are recovered.

9. Open the NetWorker Administration window in NMC and check that all of the NetWorker server resources appear as expected. [NetWorker Management Console interface on page 37](#) describes how to open the NetWorker Administration window.
  - a. Click the **Configuration** icon and check that all resources appear as expected prior to recovery.
  - b. Click the **Devices** icon and check that all devices appear as expected prior to recovery.
  - c. Click the **Media** icon and check that all media resources appear as expected prior to recovery.
  - d. Select **Disk Volumes** from the Media screen. Check the volume's *mode* status, which is shown in the window on the right. All disk volumes should have the same mode that existed prior to the recovery. All devices that will be written to should be in the appendable mode.

#### Note

If you used the `-N` or `-N -F` option with the `nsrdr` command, then all of the recovered devices will be set to the scan needed mode (displayed as Mode = Scan Needed). In this case, complete the following steps in this procedure. Otherwise, skip the following steps and resume regular operations with NetWorker.

10. If you used the `-N -F` option with the `nsrdr` command, all of the disk volumes that are appendable (non read-only) and that are listed in the recovered bootstrap's media database are set to **Scan Needed**. If you suspect that the disk volumes have save sets that were saved after the last bootstrap backup, you can run the `scanner -i` command to populate the recovered bootstrap and the client file indexes with the missing save set information.

A manual save operation is the only way a save set can get backed up without triggering a save of the bootstrap and CFI data. If a manual backup was performed before the next scheduled backup, which always backs up the bootstrap and client file indexes, then the last saved bootstrap and CFI will not have a record of the save sets that were backed up manually.

#### NOTICE

The `scanner -i` command can take a very long time to complete, especially on a large disk volume. For volumes that you do not suspect have save sets that were backed up after the last bootstrap backup or for volumes where you do not need to keep these manual backups, you can skip this step and remove the Scan Needed flag on the volume.

- For AFTD volumes that you suspect may have save sets that were saved after the last bootstrap backup, enter the following command:

```
scanner -i device_name
```

where *device\_name* is the AFTD device name not the AFTD volume name.

If you do not know the AFTD device name that corresponds to the AFTD volume, use the `nsrmm` command with the `-C` option, for example:

```
nsrmm -C
```

Output similar to the following is displayed:

```
32916:nsrmm: file disk volume_name mounted on device_name,  
write enabled
```

where *device\_name* is the device that corresponds to the AFTD *volume\_name*.

- For cloud volumes, enter the following command:

```
scanner -i -V cloud_volume -Z datazone_ID cloud_device
```

where *datazone\_ID* is the NetWorker server datazone ID if it is in a different datazone than the cloud device.

11. For AFTD devices, remove the Scan Needed status so that recover space operations are enabled for the device:

- a. Unmount the AFTD volume:

- From the NetWorker server's Administration window, click the **Devices** icon and then click **Devices** in the left panel.
- Identify the device in the right panel to be unmounted. Note the volume associated with the device.
- Right click the device and select **Unmount**.
- Repeat for all devices that require the Scan Needed status to be removed. This should be the status of all devices if `nsrdr` was used with the `-N -F` options.

- b. Remove the Scan Needed status:

- From the NetWorker server's Administration window, click the **Media** icon and then click **Disk Volumes** in the left panel.
- Identify the volume in the right panel that is associated with the device in the previous step.
- Right click the volume and select **Mark Scan Needed**.
- Select **Scan is NOT needed** and click **OK**.
- Repeat for all volumes that require the Scan Needed status to be removed.

- c. Mount the AFTD volume

- From the NetWorker server's Administration window, click the **Devices** icon and then click **Devices** in the left panel.
- Identify the device in the right panel to be mounted.
- Right click the device and select **Mount**.
- Repeat for all devices that were unmounted.
- Ensure that all devices are mounted and that the Scan Needed status has been removed for the associated volumes.

12. If you used the `-N` option with the `nsrdr` command and you attempt to mount a tape volume that has save sets that are newer than what is recorded in the media database, a message similar to the following appears:

```
nw_server nsrd media info: Volume volume_name has save sets  
unknown to media database. Last known file number in media
```

database is ### and last known record number is ###. Volume volume\_name must be scanned; consider scanning from last known file and record numbers.

- a. Make a note of the file number and record number that is displayed in the message and then enter the following command to update the media database and thus, avoid a potential loss of data:

```
scanner -f file -r record -i device
```

- b. After the scanner operation completes, remove the Scan Needed flag from the tape volume by using the nsrmm command:

```
nsrmm -o notscan volume_name
```

## Results

You can now use regular recovery procedures to recover application and user data on the NetWorker server.

### NOTICE

If the recovered NetWorker server was protecting virtual cluster clients or a NMM protected virtual DAG Exchange server, the nsrdr.log file will contain false error messages related to the CFI recovery of the underlying physical hosts. Using a NMM protected virtual DAG Exchange server as an example, you would see messages similar to the following:

```
9348:nsrck: The index recovery for 'EXCH2010-2.v111.local' failed.9431:nsrck:  
can't find index backups for 'EXCH2010-2.v111.local' on server 'sa-  
wq.v111.local'
```

You can ignore error messages related to the physical hosts because NetWorker does not backup the underlying physical host in a virtual environment.

## Options for running the nsrdr command

You can run the NetWorker server disaster recovery wizard command (nsrdr) with various command line options instead of running the wizard in fully interactive mode. The following table includes a brief description of the nsrdr command line options. For a complete description of the nsrdr command and its options, refer to the *EMC NetWorker Command Reference Guide* or the UNIX man pages.

**Table 55** Command line options for the nsrdr command

| Option                 | Description                                                                                                                                                                                                                                                                                                                                               |
|------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| -a                     | Runs the command line wizard in non-interactive mode. At a minimum, the -B and -d options must be specified with this command.<br>Be sure to specify a valid bootstrap ID with the -B option when running this command in non-interactive mode. Otherwise, the wizard will exit as though it was cancelled without providing a descriptive error message. |
| -B <i>bootstrap_ID</i> | The saveset ID of the bootstrap to be recovered.                                                                                                                                                                                                                                                                                                          |

**Table 55** Command line options for the nsrdr command (continued)

| Option                                                | Description                                                                                                                                                                                                                                                                                                                                                                                                   |
|-------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <code>-d device_name</code>                           | The device from which to recover the bootstrap.                                                                                                                                                                                                                                                                                                                                                               |
| <code>-K</code>                                       | Use the original resource files instead of the recovered resource files.                                                                                                                                                                                                                                                                                                                                      |
| <code>-v</code>                                       | Verbose mode. Generates debugging information.                                                                                                                                                                                                                                                                                                                                                                |
| <code>-q</code>                                       | Quiet mode. Display only error messages.                                                                                                                                                                                                                                                                                                                                                                      |
| <code>-c</code>                                       | Recover client file indexes only. If specified with the <code>-a</code> option, you must also specify the <code>-l</code> option.                                                                                                                                                                                                                                                                             |
| <code>-l</code><br><code>-l client1 client2...</code> | Specify which CFIs (client file indexes) to recover. Each client name must be entered on the command line and separated with a space. If no client names are specified, all client file indexes are recovered.<br>When the <code>-l</code> option is specified, ensure that it is the last option in the command string because any entries after the <code>-l</code> option are interpreted as client names. |
| <code>-f path/file_name</code>                        | Specify which CFIs to recover by using an ASCII text file. Place each client name on a separate line in the file. Must be used with the <code>-l</code> option. Ensure that each client name is entered correctly because there is no validation of client names.                                                                                                                                             |
| <code>-t date/time</code>                             | Recover CFIs from the specified date or date and time. You must enter a date and optionally, a time, format that is accepted by the <code>nsr_getdate</code> program. The <i>EMC NetWorker Command Reference Guide</i> or the UNIX man pages provide more information about <code>nsr_getdate</code> .                                                                                                        |
| <code>-N</code>                                       | If tapes have save sets that are newer than what is recorded in the recovered bootstrap backup, they will be marked as Scan Needed to prevent the possibility of losing backed up data.                                                                                                                                                                                                                       |
| <code>-F</code>                                       | Prevents recover space operations on disk devices such as AFTDs until the Scan Needed flag is removed. A recover space operation purges the disk device of any save sets that do not have a corresponding entry in the media database.<br>Must be used with the <code>-N</code> option.                                                                                                                       |

### Examples

The following examples depict some common command line usages with the `nsrdr` command and its options.

- To recover the bootstrap data and selected client file indexes only:

```
nsrdr -l client1 client2 client3
```

where each client name is separated with a space.

- To recover the bootstrap data and selected client file indexes by using an input file:

```
nsrdr -f path\file_name -l
```

where `file_name` is an ASCII text file with one client name on each line.

- To skip the bootstrap recovery and recover selected client file indexes by using an input file:

```
nsrdr -c -f path\file_name -I
```

where *file\_name* is an ASCII text file with one client name on each line.

- To skip the recovery of bootstrap data and recover all client file indexes:

```
nsrdr -c -I
```

- To skip the recovery of bootstrap data and recover selected client file indexes:

```
nsrdr -c -I client1 client2
```

- To skip the recovery of bootstrap data and recover selected client file indexes from a specified date:

```
nsrdr -c -t date/time -I client1 client2
```

where the *date/time* is the date and/or time from which the client file indexes are recovered. The date/time format is specified in *MM/DD/YYYY* format or any date and time accepted by the `nsr_getdate` command. The *EMC NetWorker Command Reference Guide* or the UNIX man pages provide more information about `nsr_getdate`.

- To run `nsrdr` in non-interactive mode and to recover the bootstrap data and all client file indexes:

```
nsrdr -a -B bootstrap_ID -d device -I
```

## Setting nsrdr tuning parameters

You can specify the following tuning parameters for the NetWorker Server Disaster recovery wizard.

- The path to the NetWorker services, such as `nsrdr`, if the default path was not used during the installation.
  - The default path on Solaris and Linux is `/etc/init.d/networker`, the default path on HPUX is `/sbin/init.d/networker`, and the default path on AIX is `/etc/rc.nsr`.
  - The default path on Windows is `C:\Program Files\EMC NetWorker\nsr\bin`
- The number of parallel threads that can be spawned when recovering CFIs (client file indexes) for multiple NetWorker clients. The default value is 5, which means that up to five parallel threads are spawned to recover CFIs. If you are recovering a large number of client CFIs, increasing this value can shorten the disaster recovery time.

If you do specify any of these parameters, they must be set up before running the wizard. You set up these parameters by creating an ASCII plain text file named `nsrdr.conf`, entering the parameter values in the file, and placing the file under the debug folder of the NetWorker installation.

### Procedure

1. Create a text file and give it the name `nsrdr.conf`.

---

**Note**

Some text editors append .txt to the end of the file name. If this occurs, remove the .txt extension so that the file name is nsrdr.conf.

2. To specify a non-default path to the NetWorker services on UNIX or Linux, add the following entry:

```
NSRDR_SERVICES_PATH = /non_default_path/nsr
```

Where non\_default\_path is the path to the NetWorker services. On Windows, the path would look similar to the following:

```
NSRDR_SERVICES_PATH = drive:\non_default_path\EMC NetWorker\nsr  
\bin
```

3. To specify the number of parallel threads that can be spawned when recovering CFIs for multiple clients, add the following entry:

```
NSRDR_NUM_THREADS = number
```

Where *number* is a value that is greater than 1. If a value of zero (0) or a negative value is entered, the default value of 5 is used instead.

Ensure that a space is added before and after the equals (=) sign. If you specify both tuning parameters, ensure that each value is entered on a separate line.

4. Save the nsrdr.conf file as a plain text file and place it in the following directory:

On UNIX or Linux: /nsr/debug/

On Windows: NW\_install\_path\nsr\debug

The tuning parameters will take effect the next time the wizard is run.

## Recovering the NMC server database

The NMC server database contains management data such as report information. The EMC NetWorker Procedure Generator provides information about recovering a NMC server database.



# CHAPTER 15

## Enterprise reporting and events monitoring

This chapter contains the following topics:

- [Enterprise data reporting](#).....390
- [Enterprise events monitoring](#).....423
- [About Events](#).....423

## Enterprise data reporting

To facilitate trend analysis, capacity planning, and problem detection, NetWorker software automatically collects data on a continual basis from the NetWorker enterprise. The NMC server stores the collected information in the Console database for a specified number of days, as described in [Data retention and expiration policies on page 391](#).

The NetWorker software then integrates and processes this data to produce a number of reports on backup status, backup statistics, events, inactive files, hosts, users, and devices. [Report categories on page 392](#) provides detailed information about the various types of reports.

The following options are available through the NetWorker Console reporting feature:

- Data collection for the entire enterprise or for specific NetWorker servers.
- Creating of various types of reports.
- User preferences for report data, such as font, size, and whether or not to use bold. This can be useful in I18N environments.
- Selection of columns to display when viewing reports in a table format, and the order in which to display them.
- The ability to save customized reports for repeated use.
- The ability to determine how long collected data should be retained.
- Only NetWorker administrators can modify these time periods.
- The ability to share reports, or restrict the sharing of reports, with other users by giving them access to the reports.
- The ability to hide shared reports of other users when listing reports.
- The ability to run reports from the command prompt.

---

### Note

The NetWorker Console is unable to generate reports when deployed in a pure IPv6 environment due to a Sybase iAnywhere 9 limitation.

---

## Enabling or Disabling the gathering of report data

The Gather Reporting Data feature is set by default when a host is added to the enterprise. If the NetWorker server to be monitored is not yet in the enterprise, you can enable the Gather Reporting Data feature when adding the NetWorker server to the enterprise. [Adding a managed host on page 482](#) provides details.

### Procedure

1. From the **Console** window, click **Enterprise**.
2. Select the **NetWorker** server for which the collection of report information is to be enabled.
3. Right-click the NetWorker managed application, then select **Properties**. The **Managed Application Properties** dialog box appears.
4. Under **Features**, select **Gather Reporting Data**, then click **OK**.

To disable the gathering of reporting data, clear the Gather Reporting Data checkbox, then click **OK**.

## Data retention and expiration policies

NetWorker Console provides separate expiration policies for retaining different types of data to meet the needs of the environment as described in this table. Only a Console Application Administrator can modify these policies.

**Table 56** Data retention policies

| Retention policy                                                                                                                                     | Type of data to be retained                                                                                                                                        | Default   |
|------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------|
| Completion Data (in Backup Status reports, except in the save set output).<br>Retention policy for completion data can affect multiple reports.      | Savegroup and save set completion data and drive data.                                                                                                             | One month |
| Completion Message (in Backup Status reports, only in the save set output).<br>Retention policy for completion messages can affect multiple reports. | Messages, such as error messages for failed save sets.                                                                                                             | Two weeks |
| Backup statistics (in all Backup Statistics reports).<br>Retention policy for backup statistics data can affect multiple reports.                    | Backup statistics, such as                                                                                                                                         | One year  |
| Audit Data (in User Audit reports).<br>Retention policy for audit data affects only audit reports.                                                   | Reports on all NetWorker tasks (except License Manager tasks) performed by specified users (but only when the NetWorker User Auditing system option is activated). | One year  |
| Recover Statistics<br>Save Set Data in Recover Statistics reports.                                                                                   | Save set records.                                                                                                                                                  | One year  |

You can view the retention policies for data to which they have access by following the first three steps in [Setting expiration policies for data retention on page 392](#). These different policies give administrators the flexibility to retain certain types of information for less time than others, as demonstrated in the following example.

---

### Note

Reports not mentioned in the above table have no retention policies.

---

### Example 1 Retention Flexibility

An administrator might want to set the completion message policy to a shorter period than the completion data policy. The precise error messages about what caused a save set backup to stop might not be relevant over a longer time period. But it might be useful to save the completion data for a somewhat longer period to help with load balancing and trends.

The longest time period (one or more years) might be a suitable selection for save set data. This data is used to generate the NetWorker Backup Statistics reports. These

**Example 1** Retention Flexibility (continued)

reports can be used to determine historical trends about backups and to help guide capacity planning.

---

**Note**

The expiration policies restrict the data that can be retrieved by NetWorker Console. In other words, reports cannot include data that is older than the data retention policy. If, for example, an administrator changed a policy expiration period from 1 year to 1 month and soon afterwards reset it to 1 year, 11 months of data would be lost. Once data is purged because of the retention policy, you can only retrieve the data by recovering the full database.

---

## Setting expiration policies for data retention

---

**Note**

Only a Console Application Administrator can perform this procedure.

---

**Procedure**

1. From the **Console** window, click **Reports**.
  2. From the **Reports** menu, select **Data Retention**. The **Data Retention** dialog box appears.
  3. For each policy, type the number of periods and select a period of time (year, month, week, day).
  4. To save the configuration of the data retention policies, click **OK**.
- 

**Note**

There must be adequate space in the Console database to hold the data. If the data retention policy settings cause the Console database to run out of storage space, it stops running. The *EMC NetWorker Installation Guide* provides information about estimating the size of the Console database.

---

## Report categories

The following table describes the various report categories included in NetWorker software. Each of these categories is discussed in detail in [Preconfigured reports on page 404](#).

Report categories appear as folders within the Reports window. These reports can be run either from the Console window or from the command prompt.

**Table 57** Report categories

| Category of report          | Purpose                                                                                                                                                                                                                                            |
|-----------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| NetWorker Backup Statistics | Provide statistical information about save sets from the media database. Include summaries of size, number of files, and number of save sets backed up. <a href="#">NetWorker backup statistics reports on page 404</a> provides more information. |

**Table 57** Report categories (continued)

| Category of report               | Purpose                                                                                                                                                                                                                                            |
|----------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| NetWorker Backup Status          | Provide status information about savegroup completion and save set backups.<br><a href="#">NetWorker backup status reports on page 406</a> provides more information.                                                                              |
| Clones                           | Provides the history of automatic and scheduled clone operations performed on NetWorker servers on version 7.6 Service Pack 2 and later. <a href="#">NetWorker clone reports on page 408</a> provides more information.                            |
| Events                           | Provide summary and detailed information about NetWorker events.<br><a href="#">Event reports on page 413</a> provides more information.                                                                                                           |
| Hosts                            | Provide a listing of NetWorker servers in the Enterprise, including information about event and reporting features. <a href="#">Host reports on page 415</a> provides more information.                                                            |
| Users                            | Provide lists of defined NetWorker Console users, logout and login reports, audit reports, and users with restricted views. <a href="#">User reports on page 415</a> provides more information.                                                    |
| Devices                          | Provide information about the way devices are being used.<br><a href="#">Device reports on page 415</a> provides more information.                                                                                                                 |
| Inactive Files                   | Manages inactive files on a client or group and sets the NetWorker software to automatically generate a list of inactive files in an environment.<br><a href="#">Inactive files on page 417</a> provides more information.                         |
| NetWorker Recover                | Provide the history of recovery operations that have been performed by NetWorker servers. <a href="#">NetWorker recovery reports on page 409</a> provides detailed information about the reports in this category.                                 |
| Avamar Statistics                | Provide deduplication backup statistics for each selected NetWorker client.<br><a href="#">Avamar Statistics reports on page 412</a> provides more information.                                                                                    |
| Cloud Backup and Recover         | Provide information on the Cloud usage for scheduled backups and recovers that are performed by the NetWorker server to and from the Cloud storage device. <a href="#">Cloud backup and recover reports on page 416</a> provides more information. |
| Data Domain Statistics           | Provides deduplication backup statistics for each selected NetWorker client.<br><i>EMC NetWorker Data Domain Deduplication Devices Integration Guide</i> provides more information.                                                                |
| NetWorker Data Protection Policy | Provides details and summaries for Data Protection Policies.<br>The <i>EMC NetWorker and VMware Integration Guide</i> provides more information.                                                                                                   |

## Report types

All of the reports are listed within the report category folders. These folders are seen in the left pane of the Reports window. Each folder contains basic and drill-down reports. [Basic reports on page 394](#) and [Drill-down reports on page 394](#) provide detailed information.

Different icons represent the different types of reports:

**Table 58** Report icons

| Icon                                                                              | Description              |
|-----------------------------------------------------------------------------------|--------------------------|
|  | Basic report             |
|  | Shared basic report      |
|  | Drill-down report        |
|  | Shared drill-down report |

## Basic reports

The basic reports organize the collected data in a manner that focuses on a specific datazone component, time span, or attribute. For example:

- A Server Summary of Backup Statistics provides backup statistics in a server-centric manner.
- A Monthly Summary of Backup Statistics provides the backup statistics in a date-centric manner.
- A Priority Summary of Events provides a report in an attribute-centric manner.

Select the basic report that best provides the information you need.

## Drill-down reports

Drill-down reports are preset sequences of basic reports, and can be saved as customized reports in shared mode.

Move up and down through a sequence to compare the information provided by the different focal points. For example, from the NetWorker Backup Status category, it is possible to select the Group Status by a Server drill-down report. This report starts at the server level, then drills down to display a summary report for each of the following:

- A selected group
- A selected monthly summary
- A selected daily summary

---

### Note

In [document mode on page 754](#) for drill-down reports, the print and export commands do not print or export the entire drill-down report, just the basic report that is currently displayed. Also note that drill-down reports cannot be run from the command prompt.

## Customized reports

A report that is included with NetWorker software is known as a [canned report on page 752](#) and includes several configuration parameters that allow the tailoring of report data. With customized reports, report versions can be configured—a single time—to fit the needs of the enterprise, and then saved and rerun whenever necessary, without having to be configured again. This saves time, especially with regularly run reports that include complex combinations of parameters. Customized reports can be run either on demand, or according to a preset schedule. The owner of a saved report can also allow it to be shared with all users.

The Hide Other Users Reports option toggles the view of reports between:

- The owner's reports (private and shared)
- The owner's reports, plus all shared custom reports

[Customizing and saving reports on page 418](#) and [Sharing reports on page 419](#) provide more information.

## How to configure reports

Each type of report includes its own configuration parameters that act as filters limiting the data used to build the report output. By default, these parameters are set to include all the information available in the report, which means that the filters are turned off to begin with.

For example, the NetWorker Backup Statistics Server Summary report includes these configuration parameters:

- Server name
- Backup type
- Backup level
- Save time

In this example, accepting the default configuration of selected parameters results in a report that includes backup statistics for all the servers in the enterprise. The statistics reported for each server would include all backup types and levels, and the time range would include all the data available.

### Note

For Drive Utilization reports, the time range cannot exceed eight days. [Date and time formats on page 396](#) provide more information about this limitation, or for details on how to set this range.

The scope of a report can be limited by filtering out one or more parameter options, for example:

- To exclude certain servers in the enterprise from the report, remove selected server names from the Server Name Selected box.
- To select only full backups, remove the other backup types from the Server Name Selected box.
- To include only the statistics for the past month, specify that time range. Time ranges are localized. The input format follows the format specified in locale settings of the operating system.

When a parameter is removed from the Server Name Selected box, it goes into the Server Name Available box. To include that parameter again, click Add ().

## Configuring a report

### Note

If you receive the error **com.sybase.jdbc3.jdbc.SybDriver** when you generate a report, close the Console server window, clear the Java Cache on the Console client, then generate the report again. The *EMC NetWorker Installation Guide* describes how to clear the Java Cache.

### Procedure

1. From the **Console** window, click **Reports**.
2. Expand a report category folder, then select an available report type.
  - When a report type has been selected, the **Configure** tab for that report appears in.
  - The possible parameters for that report appear by default in the **Selected** boxes.
3. To limit the scope of the report, click any of the parameters in the **Selected** box, then click **Remove** (  ).
- To remove all of the parameters from the **Selected** box, click **Remove All** (  ).
- Removed parameters appear in the **Available** boxes.
4. To return:
  - A single parameter to the **Selected** box, select it from the **Available** box and click **Add** (  ).
  - All available parameters to the **Selected** box, click **Add All** (  ).
5. To display the report, select the **View Report** tab.

### Date and time formats

If a report includes a date-and-time-range parameter, specify the beginning and end date and time in the To and From text boxes. Clicking the arrow of a time input field displays a calendar and clock selector, including adjustment arrows for setting values.

In US English locales, the default “From” hour is 12:00:00 (midnight/morning) on the “From” date, and the default “To” hour is 11:59:59 (night) on the “To” date. The US English locale is the only one that includes a box for an A.M. or P.M. value.

In non-US English locales, the default “From” hour is 00:00:00 (midnight/morning) on the “From” date, and the default “To” hour is 23:59:59 (night) on the “To” date.

The option of displaying times in 12- or 24-hour formats is determined by the Regional and Language Settings on the system.

### Input formats

Date and time input formats in the NetWorker software vary. Some acceptable input formats for a collection of common locales are shown in this table.

**Table 59** Date and time input formats for common locales

| Language   | Date formats                                                                                                                                                                                           | Time formats                                                                                                                                            |
|------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------|
| US English | <ul style="list-style-type: none"> <li>• EEEE, MMMM D, YYYY (Monday, March 8, 2009)</li> <li>• MMMM D, YYYY (March 8, 2009)</li> <li>• MMM D, YYYY (Mar 8, 2009)</li> <li>• M/D/YY (3/8/07)</li> </ul> | <ul style="list-style-type: none"> <li>• h:mm:ss a z (11:27:30 P.M. PST)</li> <li>• h:mm:ss a (11:27:30 P.M.)</li> <li>• h:mm a (11:27 A.M.)</li> </ul> |
| UK English | <ul style="list-style-type: none"> <li>• DD MMMM YYYY 08 March 2009</li> </ul>                                                                                                                         | <ul style="list-style-type: none"> <li>• HH:mm:ss z (23:27:30 PST)</li> </ul>                                                                           |

**Table 59** Date and time input formats for common locales (continued)

| Language           | Date formats                                                                                                                                                                                          | Time formats                                                                                                                          |
|--------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------|
|                    | <ul style="list-style-type: none"> <li>• DD-MMM-YYYY (08-Mar-2009)</li> <li>• DD/MM/YY (08/03/07)</li> </ul>                                                                                          | <ul style="list-style-type: none"> <li>• HH:mm:ss (23:27:30)</li> <li>• HH:mm (23:27)</li> </ul>                                      |
| French             | <ul style="list-style-type: none"> <li>• EEEE D MMMM YYYY (lundi 8 mars 2009)</li> <li>• D MMMM YYYY (8 mars 2009)</li> <li>• D MMM YYYY (8 mar. 2009)</li> <li>• DD/MM/YY (08/03/07)</li> </ul>      | <ul style="list-style-type: none"> <li>• HH:mm:ss z (23:27:30 PST)</li> <li>• HH:mm:ss (23:27:30)</li> <li>• HH:mm (23:27)</li> </ul> |
| German             | <ul style="list-style-type: none"> <li>• EEEE, D. MMMM YYYY (Montag, 8. März 2009)</li> <li>• D. MMMM YYYY (8. März 2009)</li> <li>• DD.MM.YYYY (08.03.2009DD)</li> <li>• MM.YY (08.03.07)</li> </ul> | <ul style="list-style-type: none"> <li>• HH:mm:ss z (23:27:30 PST)</li> <li>• HH:mm:ss (23:27:30)</li> <li>• HH:mm (23:27)</li> </ul> |
| Japanese           | <ul style="list-style-type: none"> <li>• YYYY/MM/DD (2009/03/08)</li> <li>• YY/MM/DD (07/03/08)</li> </ul>                                                                                            | <ul style="list-style-type: none"> <li>• HH:mm:ss z (23:27:30 JST)</li> <li>• HH:mm:ss (23:27:30)</li> <li>• HH:mm (23:27)</li> </ul> |
| Simplified Chinese | <ul style="list-style-type: none"> <li>• YYYY-M-D (2009-3-8)</li> <li>• YY-M-D (07-03-8)</li> </ul>                                                                                                   | <ul style="list-style-type: none"> <li>• HH:mm:ss (23:27:30)</li> </ul>                                                               |

Note that in the previous table:

- Formats shown as single digits (M, D, h) may also be entered as double digits. For example, M could be either 7 or 07 for the seventh month.
- In the time-formats column:
  - The **a** character denotes a 12-hour format.
  - The absence of an **a** character denotes a 24-hour format.
  - The **z** character indicates time zone. If the **z** is present, then the output time will contain a time zone.

Relative times can also be entered in the From and To fields. A valid relative time consists of a number followed by a unit of time, for example, *2 months*. Time units can include Hour, Day, Week, Month, and Year.

Remember that these reports are run by using dates that have already occurred. Consequently, even the *To* date is always a past date. The relative time *4 months* would provide report data covering the past 4 months. A report specifying *from 9 months to 1 month* includes data from nine months ago up to one month ago.

#### Note

For Drive Utilization reports, the time range cannot exceed 8 days. That is, the date entered in the To field cannot exceed 8 days from the date entered in the From field. If typing a relative time in the To field, the value cannot exceed 8 days.

## How to view reports

Before displaying a report, select the scope of the report by specifying Configuration parameters. [Configuring a report on page 395](#) provides information on configuring reports.

In addition, reports can be printed or exported to various file formats. [Printing reports on page 423](#) and [Exporting reports on page 420](#) provide information about printing and exporting.

The administrative user can restrict a user's view of the enterprise to certain servers, affecting the user's view and scope of his or her reporting.

### Viewing reports

Reports can be displayed in either interactive or document mode. Depending on the report, you may also select to display the content of the report as a table or as a chart. NetWorker supports the following report modes:

- [Interactive mode on page 398](#)
- [Document mode on page 400](#)
- [Interactive and document mode chart types on page 401](#)

In addition, NetWorker includes these restrictions and processing considerations:

- [Restricted report views on page 403](#)
- [Background processing of reports on page 404](#)

### Procedure

1. From **Console** window, click **Reports**.
2. Select a report type.
3. To limit the scope of the report, specify parameters on the **Configuration** tab.
4. Click the **View Report** tab. Most reports display initially in interactive mode and table format.
5. To modify the current view, right-click on the **View Report** tab and select the appropriate view option.

### Interactive mode

Interactive mode displays a report with dynamic components. The effect of the dynamic components depends on whether a report is viewed as a table or as a chart.

Interactive mode allows access to drill-down reports. Drill-down reports conveniently group related reports to make it easier to view increasing levels of granularity in report data.

Interactive Mode also offers a set of chart selection choices. These choices limit the data in a report by including or excluding certain parameters. Examples of chart-selection parameters include:

- Duration
- Save set size
- Number of files
- Amount of data
- Number of save sets

Not all parameters apply to each chart type.

## Interactive mode table view

In the table view of the interactive mode, you can:

- Scroll through rows of the table.
  - Sort, rearrange, or resize columns in the table.
  - Choose which columns to display, and the order in which to display them.
- 

### Note

In interactive mode, tables can be sorted just as they can be sorted within other Console windows.

## Interactive mode chart view

---

When a chart is displayed in interactive mode, you can:

- Switch back and forth between different chart formats by selecting a format from the Chart Type list.
- 

### Note

When viewing a Drive Utilization report as a chart, it automatically displays as a Gantt chart. The chart type cannot be changed.

- Change selections by using the Data Selector, where applicable. The Data Selector is available in select reports, and includes control-column information that works in conjunction with a graph of numerical data. While the Data Selector is useful in table format, it can also be used to display interesting and useful data groupings in chart format.

For example, in a Group Summary by Server report displayed in Bar Chart format, the bar chart displays the amount of data in each group, and the Data Selector lists the "Server" control column, making it possible to see—in one place—a summary of groups across all servers, simply by moving through the list of servers in the Data Selector. This could be useful for finding the group that backed up the most data, or for balancing groups on servers.

- Limit the set of X and Y axes in the report by clearing one or more options from the Chart Selector checkboxes. This does not apply to Drive Utilization reports.
  - For Drive Utilization reports, hover over a chart in Save Set view or Drive view to display a tool tip that includes this information:
    - Drive (Drive view only)
    - Save Set Name (Save Set view only)
    - Start Time
    - End Time
    - Client Name
    - Throughput (B/Sec)
- 

### Note

The tool tip feature for Drive Utilization reports is available only in Interactive mode.

## Document mode

Document mode displays a static report that resembles the view in Print Preview as shown by a PDF file viewer. Within Document mode, these options are available:

- Orientation (portrait or landscape)
- Table or chart format
- Size (zoom level)

---

### Note

In Document mode, for any chart type that displays *X-Y* axes, two graphs are displayed. If the top graph contains excessive *Y*-axis data, the data displayed in both graphs could be truncated.

In Document mode, the columns of a tabular report cannot be sorted, rearranged, or resized. In addition, you cannot choose which columns to display, and the order in which to display them. Likewise, the chart format cannot be modified while viewing a report. NetWorker software does not maintain any customized changes made while displaying a report in interactive mode (such as sorting or rearranging the columns in a table), except for charts (in Chart Type and Chart Selector). Instead, document mode displays the report in a standard table or chart format, as specified by the internal report definition within NetWorker software.

Unlike Interactive Mode, which offers a set of parameters for chart selection that limit the data that is displayed, a report in Document mode displays all of the data. As a result, report views in Document mode often consist of several screens. For this reason, the viewing choices in Document mode include these options for paging through the output:

- First
  - Previous
  - Next
  - Last
- Document mode table view

Document-mode reports displayed as a table contain several columns of information:

- One or more control columns represent report information that cannot be summed as quantitative data (for example, Server name, Save set name, Backup type, and so on). The control columns topics are generally shown as X-axis data in charts.
- One or more data columns represent report information that can be summed as quantitative data (for example, Amount of data, number of files, number of save sets, and duration). The data columns topics are generally shown as Y-axis data in charts.

The bottom line of each report gives subtotals and totals of all the columns of quantitative data shown in the report.

For example, a report on Save Set Details by Client:

- Lists each client.
- Provides:
  - Subtotals of the data columns for each of that client's save sets.
  - Totals of all the data columns for each client.
  - Totals of the data for all clients in the report.

This makes it easy to parse the data, visually, on a per-client basis, on a save set-per-client basis, and for all clients in the report.

## Interactive and document mode chart types

These chart types are available in both interactive and document mode:

- Bar chart
- Pie chart
- Plot chart
- Stacking bar chart
- Gantt chart (for Drive Utilization reports only -- more information is provided in the section [Device reports on page 415](#)).

When displaying reports in chart format, the size and appearance of the chart may differ depending on the orientation (portrait or landscape) and the presentation format—that is, whether viewing it in the Console window, or in other file formats, such as PDF, HTML, or PostScript. When displaying reports as charts in document mode, or when printing or exporting to HTML or PostScript, the charts are always displayed on a single page, regardless of their size. As a result, some data and labels may not display. To see full report details, view the chart in interactive mode.

The following table shows a simplified version of chart format options.

**Table 60** Report chart formats

| Format       | Example |
|--------------|---------|
| Bar          |         |
| Plot         |         |
| Pie          |         |
| Stacking Bar |         |
| Gantt        |         |

Bar chart

A bar chart uses bars to illustrate the different types of data. For example, in a bar chart of a NetWorker Backup Statistics Server Summary report, the vertical bars show the amount of data backed up by each server. The additional lines show the corresponding numbers of files and save sets backed up by each server.

The set of axes displayed in the report depends on the type of report.

To select various elements for display, select or clear the appropriate checkboxes in the Chart Selector.

#### Plot chart

Plot charts display data graphed as points along X and Y axes.

To select various elements for display, select or clear the appropriate checkboxes in the Chart Selector.

#### Pie chart

Pie charts display data graphically as a percentage of a circular “pie.” When specifying this chart type from the Console window, the Chart Selector includes a radio button that allows the display of only one element, or axis, at a time. If an additional element is selected, it replaces the first. This limitation does not occur when this chart type is specified from the command prompt:

- When this chart type is selected from the Console window, all applicable data axes are shown.
- When this chart type is specified from the command prompt, only the requested information is included.

#### Stacking bar chart

The stacking bar charts are most appropriate for reports where the data is grouped and measured according to more than one category. For example, use of a stacking bar chart to display a report that measures data according to only a single point of focus would display just a simple bar chart. Stacking bar chart reports generally include by in the name, such as by date or by host.

In Interactive mode, movement of the cursor over a section of stacked color causes a pop-up legend to appear. The legend describes the data represented by that color. This chart type is inappropriate for complicated data in Document mode, since the cursor does not display a legend describing the data represented by that color. Instead, in Document mode, select a different chart type (bar, pie, or plot) if the report data is complicated.

When specifying this chart type from the Console window, the Chart Selector includes a radio button that enables the display of only one element, or axis, at a time. If an additional element is selected, it replaces the first. This limitation does not occur when this chart type is specified from the command prompt.

- When this chart type is specified from the Console window, all applicable data axes are shown.
- When this chart type is specified from the command prompt, only the requested information is shown.

The following example describes appropriate use of the stacking bar chart type.

#### Appropriate usage of the stacking bar chart

To appreciate the different ways in which a stacking bar chart may be used, consider these reports:

- A NetWorker Backup Statistics Group Summary by Server shows statistics broken down by savegroup for each server. Different blocks of color are used for the amounts of data backed up by each savegroup within the vertical bars that represent the amount of data that are backed up by servers.

- A NetWorker Backup Statistics Server Summary shows data from only one focus, a server-centric point of view. If a stacking bar chart is selected to display a NetWorker Backup Statistics Server Summary, the chart would display solid bars of color to represent the servers. There would, however, be no blocks of color within the bars, because the report focuses only on the server level. The result would therefore look like a simple bar chart.
- Gantt chart

When viewing a Drive Utilization report as a chart, it automatically displays as a Gantt chart, and the chart type cannot be changed. The Drive Utilization report is the only report that displays as a Gantt chart.

In Save Set view, the X axis displays the time, and the Y axis displays save set data. Hovering over the chart in Save Set view displays a tool tip that provides this information:

- Save set name
- Start time
- End time
- Client name
- Throughput value

In Drive view, the X axis displays the time, and the Y axis displays drive data. Hovering over the chart in Drive View displays a tool tip that provides this information:

- Drive
  - Start time
  - End time
  - Throughput value
- Chart axis selection

Document mode can display more than one chart in the document. Any or all available Y axes can be inserted into the report. When a user changes to document mode, prints or exports a report, or saves a configuration, the axis selection currently set in the Chart Selector section of the Configuration tab is used.

The exceptions to this are stacked bar and pie charts, which display all axes when the `gstclreport` command is used to generate a report.

## Restricted report views

When a NetWorker Console user is added or reconfigured, the user's views of NetWorker servers, groups, and clients within the enterprise determines the content of reports that he or she can produce.

Since each user can have different access restrictions, the view of each report can potentially be different. This applies to all report types, whether customized, private, or shared.

For example, a shared backup summary report entitled "Building C Backups" will show different data for different users if the users' access permissions include different NetWorker servers. This is so even if the reports are run at the same time.

In the Reports function, report parameters for a specific user display only the allowed NetWorker servers, groups, and clients as sources of report information. The resulting reports contain data only from those servers. A user may only run reports for servers he or she is allowed to manage.

---

**Note**

If no data is available for a given server, that server will not appear in any lists, regardless of the user's view or access.

---

## Background processing of reports

When the View Report tab is selected, the report data is removed from the server. This process happens in the background and could take awhile. Other portions of the interface are usable while the report data is being processed. The requested report appears upon returning to the View tab.

**NOTICE**

Do not request multiple reports at the same time. Since reports are run sequentially in the background, a user can navigate around in the user interface while a report is running. If a new report is started before an earlier report is finished, then the earlier report is terminated and deleted. A report is either complete or deleted, the results are never partial.

---

## Preconfigured reports

NetWorker software includes a variety of reports:

- [NetWorker backup statistics reports on page 404](#)
- [NetWorker backup status reports on page 406](#)
- [NetWorker clone reports on page 408](#)
- [NetWorker recovery reports on page 409](#)
- [Data Domain statistics reports on page 411](#)
- [Avamar Statistics reports on page 412](#)
- [Event reports on page 413](#)
- [Host reports on page 415](#)
- [User reports on page 415](#)
- [Device reports on page 415](#)
- [Cloud backup and recover reports on page 416](#)
- [Inactive files on page 417](#)

### NetWorker backup statistics reports

The different types of reports included within the NetWorker Backup Statistics report category provide backup statistics for each selected NetWorker server within the enterprise.

NetWorker Backup Statistics reports may include this information:

- Amount of data backed up.
- Number of files backed up.
- Number of save sets backed up.

Types of NetWorker backup statistics reports and configuration

The NetWorker Backup Statistics report category includes basic and drill-down reports.

The Configure tab allows you to limit the scope of the report that was selected.

The parameters available within the NetWorker Backup Statistics report category are described in this table. The specific parameters available depend on which NetWorker Backup Statistics report is selected.

**Table 61** NetWorker backup statistics parameters

| Parameter     | Description                                                                                                                                                                                       | Options                                                                              |
|---------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------|
| Server Name   | Selects managed hosts within the enterprise.                                                                                                                                                      | Selected server names                                                                |
| Group Name    | Selects one or more groups.                                                                                                                                                                       | Selected group names                                                                 |
| Client Name   | Selects one or more clients.                                                                                                                                                                      | Selected client names                                                                |
| Save Set Name | Selects one or more save sets.                                                                                                                                                                    | Selected save set names                                                              |
| Backup Type   | Selects one or more file types.                                                                                                                                                                   | List of supported file types                                                         |
| Level         | Select one or more backup levels.                                                                                                                                                                 | List of backup levels such as, Full, Incremental, Skip, synthetic full, or Level 1-9 |
| Save Time     | Limits the report to a specified time range. The default range is one day for save set details reports.<br>The date/time format available depends on the language locale of the operating system. | Save time (range)                                                                    |

The parameters available for each report type in the NetWorker Backup Statistics report category are listed in the user interface.

#### Save set data retention policy and configuration

Settings for the save set retention policy impact the data that is available to the NetWorker Backup Statistics reports. If a save set retention policy of 6 months is specified, NetWorker software cannot query the database for a time range that extends back more than 6 months. The report cannot display data that has expired because that data has been removed from the database. Thus, even if a save time parameter of one year is specified, the report can display only six months of data if the limit of the save set retention policy is six months.

#### Backup statistics basic reports

Within the NetWorker Backup Statistics report category, choose any of the basic reports listed in the user interface. Once a report is chosen, the Configuration tab displays boxes with lists of the selected parameters for that report. To exclude unwanted parameters from the report, delete them from the list. [Configuring a report on page 395](#) provides information on selecting and removing parameters.

Except for the Avamar Backup Summary report, these basic reports do not distinguish between regular and deduplication clients.

#### Backup statistics drill-down reports

The drill-down reports consist of multiple NetWorker Backup Statistics basic reports, connected in a predetermined sequence. [Drill-down reports on page 394](#) provides general information about drill-down reports.

The configuration parameters for a drill-down report are the same as the parameters for the top-level report in the report sequence. Thus, if the top layer of the drill-down report is a Monthly Summary report, the configuration parameters are the same as they would be for the basic report, Monthly Summary.

When a report is chosen, the Configuration tab displays boxes that list the selected parameters for the top-level report. To exclude unwanted parameters from the report, delete them from the list. [Configuring a report on page 395](#) provides information on selecting and removing parameters.

## NetWorker backup status reports

The NetWorker Backup Status reports consolidate information about the success of scheduled group backups. As with the NetWorker Backup Statistics reports, these reports can provide either an enterprise-wide or a more focused summary of activity over a specified time range.

The NetWorker Backup Status reports provide the same basic function as selecting Show Details for a group in the Monitoring window of the Administration window. The NetWorker Backup Status reports, however, allow you to select the scope and level of detail.

The report calculates the amount of time taken by each backup group individually. Consequently, if several groups run in parallel, their total combined backup time is greater than the time elapsed between the start of the first group and the completion of the last group. For example:

- Group A starts at 13:00 and completes at 15:00.
- Group B starts at 13:30 and completes at 15:30.

Although the groups both completed within a 2.5-hour period, the total group runtime is counted as 4 hours.

NetWorker Backup Status reports can include this information:

- Total group runs
- Totals of successful, failed, and interrupted group runs
- Success ratio
- Backup duration
- Backup level
- Backup type
- Save type

These backup status reports cover both regular and deduplication clients.

### Backup type and save type information

Backup type is one of the configuration parameters for both NetWorker Backup Statistics and NetWorker Backup Status reports, and it is one of the fields of information included in these reports. The backup type indicates whether the files backed up were regular files, bootstrap files, indexes, or a particular database file.

Specialized NetWorker modules (such as NetWorker Module for SAP) are used to back up the various databases. Most of these modules apply a distinct prefix when backing up a save set. This prefix enables NetWorker software to identify the backup type and include it in the reports.

A couple of the Backup Status reports (Save Set Details and Save Set Details by Client) include an additional field of information called save type. The save type can be any one of the following:

- Bootstrap
- Index
- Save

- Save (backup command)

Types of NetWorker backup status reports and configuration

The NetWorker Backup Status Report category includes both basic and drill-down reports. The report's Configure tab allows you to limit the scope of the report selected. The choice of available parameters depends on which report is to be generated.

The parameter options available within the NetWorker Backup Status Report category are described in this table.

**Table 62** NetWorker backup status parameters

| Parameter        | Description                                                                                             | Options                                                                                                                                            |
|------------------|---------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------|
| Server Name      | Selects one or more NetWorker servers.                                                                  | Selected server names                                                                                                                              |
| Group Name       | Selects one or more savegroups.                                                                         | Selected group names                                                                                                                               |
| Group Start Time | Limits the report to a specified time range. The default range is one day for save set details reports. | Start and end dates                                                                                                                                |
| Client Name      | Selects one or more clients.                                                                            | Selected client names                                                                                                                              |
| Save Set Name    | Selects one or more save sets.                                                                          | Selected save set names                                                                                                                            |
| Backup Type      | Selects one or more file types.                                                                         | List of supported file types.                                                                                                                      |
| Level            | Selects one or more backup levels.                                                                      | <ul style="list-style-type: none"> <li>• Full</li> <li>• Incremental</li> <li>• Skip</li> <li>• Level 1-9<br/>(Partial list of options)</li> </ul> |
| Status           | Selects status.                                                                                         | <ul style="list-style-type: none"> <li>• Successful</li> <li>• Failed</li> <li>• Interrupted</li> </ul>                                            |

The parameters available for each report type are listed in the user interface.

#### Completion data retention and NetWorker backup status

The settings for the completion data policy impact the data that is available to the NetWorker Backup Status reports. The report cannot display data that has expired, because it has been removed from the database.

Thus, even if a one-year time range is specified for the Group Start Time parameter, the report displays only six months if the limit of the completion data policy is six months.

#### Backup status basic reports

Within the NetWorker Backup Status report category, choose any of the basic reports listed in the user interface. When a report has been chosen, the Configuration tab displays boxes listing the selected parameters for that report. To exclude unwanted parameters from the report, remove them from the list. [Configuring a report on page 395](#) provides information on selecting and removing parameters.

#### Backup status drill-down reports

The drill-down reports are comprised of multiple NetWorker Backup Status basic reports, connected in a predetermined sequence. [Drill-down reports on page 394](#) provides general information about drill-down reports. When a report has been chosen, the

Configuration tab displays boxes with lists of the selected parameters for the top-level report. Thus, if the top layer of the drill-down report is a Daily Summary report, the configuration parameters are the same as they would be for the basic report, Daily Summary.

To exclude unwanted parameters from the report, remove them from the list. [Configuring a report on page 395](#) provides information on selecting and removing parameters.

## NetWorker clone reports

The Clone reports, available from the Reports task pane in the Console window, allow you to view the history of automatic and scheduled clone operations that have been performed by NetWorker servers for any server version 7.6 Service Pack 2 and later.

Four different types of clone reports can be generated:

- Server Summary
- Clone Details
- Save Set Details
- Clone Summary Over Time

Be aware that clone reports may not be up-to-date because clone records are gathered by the console server every 12 hours.

### Types of NetWorker clone reports and configuration

The NetWorker clone report category includes basic and drill-down reports for each selected NetWorker server within the enterprise. The Configuration tab allows you to limit the scope of the report that was selected.

The parameters available for clone reports are described in this table. The specific parameters available depend on which clone report is selected.

**Table 63** Clone report parameters

| Parameter        | Description                                               | Options                                                                                                                                            |
|------------------|-----------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------|
| NetWorker Server | Select one or more NetWorker servers.                     | Selected server names                                                                                                                              |
| Client Name      | Name of the NetWorker client whose save sets were cloned. | Selected client names                                                                                                                              |
| Clone Name       | Name of the scheduled clone resource used for cloning.    | Selected clone resource                                                                                                                            |
| Save Set         | Cloned saveset name.                                      | Selected save set names                                                                                                                            |
| Level            | Backup level of the clone.                                | <ul style="list-style-type: none"> <li>• Full</li> <li>• Incremental</li> <li>• Skip</li> <li>• Level 1-9<br/>(Partial list of options)</li> </ul> |
| Status           | Final completion status of the clone.                     | <ul style="list-style-type: none"> <li>• Successful</li> <li>• Failed</li> <li>• No save sets found</li> </ul>                                     |
| Type             | Type of clone operation.                                  | <ul style="list-style-type: none"> <li>• Scheduled</li> </ul>                                                                                      |

**Table 63** Clone report parameters (continued)

| Parameter        | Description                                                                                                                                                                                       | Options                                                  |
|------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------|
|                  |                                                                                                                                                                                                   | <ul style="list-style-type: none"> <li>Manual</li> </ul> |
| Start / End Time | Limits the report to a specified time range. The default range is one day for save set details reports.<br>The date/time format available depends on the language locale of the operating system. | Start time of clone<br>End time of clone                 |

### Clone basic reports

Within the Clone report category, choose any of the basic reports listed in the user interface. Once a report is chosen, the Configuration tab displays boxes with lists of the selected parameters for that report. To exclude unwanted parameters from the report, remove them from the list. [Configuring a report on page 395](#) provides information on selecting and removing parameters.

### Clone drill-down reports

The Clone Summary over Time drill-down report consists of the basic clone reports, connected in a predetermined sequence. [Drill-down reports on page 394](#) provides general information about drill-down reports.

The configuration parameters for the drill-down report are the same as the parameters for the Server Summary basic clone report.

To generate the Clone Summary Over Time report, first specify the same parameters as those in the Server Summary clone report, which will be the first report displayed in the sequence.

To drill down to the clone detail level, perform one of the following, depending on your viewing mode:

- When in Table mode, double-click on any individual row referencing the desired NetWorker server.
- When in Chart mode, click anywhere in the chart area of the desired NetWorker server.

The Clone Details report for the selected NetWorker server appears. Return to the Server Summary report to select another server to explore.

To drill down to the Save Set Details level, perform one of the following, depending on your viewing mode:

- When in Table mode, double-click on any individual row referencing the desired clone resource name.
- When in Chart mode, click anywhere in the chart area of the desired clone resource name.

The Save Set Details report for the selected clone resource appears. Return to the Clone Details report to select another client to explore.

### NetWorker recovery reports

The Recovery reports, available from the Reports task pane in the Console window, allow you to view the history of recovery operations that have been performed by NetWorker servers for any server version 7.3 and later. Additionally, NMC checks for new recovery

operations and stores the recover statistics in the Console database every 12 hours and every time a scheduled savegroup backup completes.

Reports can be viewed in both Chart and Table modes, with the Table mode set as the default mode. Four different types of recover reports can be generated:

- Server Summary
- Client Summary
- Recover Details
- Recover Summary Over Time

Be aware that recovery reports may not be up-to-date because recover job history is gathered by the console server every 12 hours and on completion of every scheduled backup.

#### Types of NetWorker recovery reports and configuration

The NetWorker recovery report category includes basic and drill-down reports. The different types of reports included within the NetWorker Recover Statistics report category provide recover statistics for each selected NetWorker server within the enterprise.

The Configuration tab allows you to limit the scope of the report that was selected.

The parameters available within the NetWorker Recovery report category are described in this table. The specific parameters available depend on which NetWorker Recovery Statistics report is selected.

**Table 64** NetWorker recovery statistics parameters

| Parameter           | Description                                                                                                                            | Options                                                                          |
|---------------------|----------------------------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------|
| NetWorker Server    | Managed hosts within the enterprise.                                                                                                   | Selected server names                                                            |
| Source Client Name  | One or more clients whose data is being recovered.                                                                                     | Selected client names                                                            |
| Target Client       | The client where the data is being recovered to.                                                                                       | Selected target client names                                                     |
| Initiating Client   | The client that initiated the recover.                                                                                                 |                                                                                  |
| User                | Name of the user who initiated the recover.                                                                                            | Selected usernames                                                               |
| Size                | The size of the recover                                                                                                                |                                                                                  |
| Number of files     | For file system recoveries, the number of files in the recover.                                                                        |                                                                                  |
| Start time/End time | Limits the report to a specified time range.<br>The date/time format available depends on the language locale of the operating system. | Start time of recover<br>End time of recover                                     |
| Completion Status   | Final status of the recover                                                                                                            | <ul style="list-style-type: none"> <li>• Successful</li> <li>• Failed</li> </ul> |

The parameters available for each report type in the NetWorker Recovery Statistics report category are listed in the user interface.

#### Recovery Statistics basic reports

Within the NetWorker Recovery Statistics report category, choose any of the basic reports listed in the user interface. Once a report is chosen, the Configuration tab displays boxes with lists of the selected parameters for that report. To exclude unwanted parameters

from the report, delete them from the list. [Configuring a report on page 395](#) provides information on selecting and removing parameters.

#### Recovery Statistics drill-down report

This drill-down report consists of multiple NetWorker Recovery Statistics basic reports, connected in a predetermined sequence. [Drill-down reports on page 394](#) provides general information about drill-down reports.

The configuration parameters for a drill-down report are the same as the parameters for the top-level report in the report sequence. Thus, if the top layer of the drill-down report is a Server Summary report, the configuration parameters are the same as they would be for the basic report, Server Summary.

When a report is chosen, the Configuration tab displays boxes that list the selected parameters for the top-level report.

To exclude unwanted parameters from the report, delete them from the list. [Configuring a report on page 395](#) provides information on selecting and removing parameters.

#### Recover Summary Over Time

Recover Summary Over Time is a drill-down report sequence that allows you to explore the history of recover jobs that were performed by NetWorker servers over a period of time.

To generate the Recover Summary Over Time report, you must first specify the same parameters as those in the Server Summary report, which will be the first report displayed in the sequence.

To drill down to the client level, perform one of the following, depending on your viewing mode:

- When in Table mode, double-click on any individual row referencing the desired NetWorker server
- When in Chart mode, click anywhere in the chart area of the desired NetWorker server.

The Client Summary report for the selected NetWorker server appears. Return to the Server Summary report to select another server to explore.

To drill down to the Recover Details level, perform one of the following, depending on your viewing mode:

- When in Table mode, double-click on any individual row referencing the desired NetWorker client
- When in Chart mode, click anywhere in the chart area of the desired NetWorker client

The Recover Details report for the selected NetWorker client appears. Return to the Client Summary report to select another client to explore.

#### Recovery data retention policy and configuration

The retention policy for the recover statistics used to generate these reports can be set with the other retention policies currently defined from the Data Retention page in the Reports task pane. The default retention policy for these statistics is 1 year.

## Data Domain statistics reports

The Data Domain reports, available from the Reports task pane in the Console window, provide Data Domain deduplication backup statistics for each selected NetWorker client.

The *EMC NetWorker Data Domain Deduplication Devices Integration Guide* provides more information.

## Data Protection Policy reports

The Data Protection policy reports, available from the Reports task pane in the Console window, provides details and summaries for Data Protection Policies.

The *EMC NetWorker and VMware Integration Guide* provides more information.

## Avamar Statistics reports

The NetWorker Avamar Statistics reports, available from the Reports task pane in the Console window, provide deduplication backup statistics for each selected NetWorker client.

Reports can be viewed in Table mode. There are four different types of reports that can be generated from the deduplication statistics:

- Client Summary
- Save Set Summary
- Save Set Details
- Backup Summary

Types of Avamar Statistics reports and configuration

The Avamar Statistics report category includes basic and drill-down reports.

The Configure tab allows you to limit the scope of the report that was selected.

The parameters available within the NetWorker Deduplication Statistics report category are described in this table. The specific parameters available depend on which NetWorker Deduplication Statistics report is selected.

**Table 65** Avamar Statistics parameters

| Parameter     | Description                                                                                                                                                                                    | Options                                                                                                                                            |
|---------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------|
| Server Name   | Selects one or more servers                                                                                                                                                                    | Selected server names                                                                                                                              |
| Client Name   | Selects one or more clients.                                                                                                                                                                   | Selected client names                                                                                                                              |
| Group Name    | Selects one or more groups                                                                                                                                                                     | Selected group names                                                                                                                               |
| Save Set Name | Selects one or more save sets.                                                                                                                                                                 | Selected save set names                                                                                                                            |
| Save Time     | Limits the report to a specified time range. The default range is one day for save set details reports. The date/time format available depends on the language locale of the operating system. | save time (range)                                                                                                                                  |
| Backup Level  | Select one or more backup levels.                                                                                                                                                              | <ul style="list-style-type: none"> <li>• Full</li> <li>• Incremental</li> <li>• Skip</li> <li>• Level 1-9<br/>(Partial list of options)</li> </ul> |

The parameters available for each report type in the Avamar Statistics report category are listed in the user interface.

Avamar Statistics basic reports

Within the Avamar Statistics report category, choose any of the basic reports listed in the user interface. Once a report is chosen, the Configure tab displays boxes with lists of the

selected parameters for that report. To exclude unwanted parameters from the report, delete them from the list. [Configuring a report on page 395](#) provides information on selecting and removing parameters.

#### Avamar Statistics drill-down reports

The drill-down report, Backup Summary, consists of multiple NetWorker deduplication Statistics basic reports, connected in a predetermined sequence. [Drill-down reports on page 394](#) provides general information about drill-down reports.

The configuration parameters for the drill-down report are the same as the parameters for the top-level report in the report sequence. Thus, if the top layer of the drill-down report is a Client Deduplication Summary report, the configuration parameters are the same as they would be for the basic report, Client Deduplication.

When a report is chosen, the Configure tab displays boxes that list the selected parameters for the top-level report. To exclude unwanted parameters from the report, delete them from the list. [Configuring a report on page 395](#) provides information on selecting and removing parameters.

## Event reports

These reports provide summary information about current events on NetWorker, Avamar, and Console servers within the Enterprise. Additional details about a particular event can be displayed, including annotation contents. While the Events window within the NetWorker Console displays the current events of the NetWorker servers (and Avamar server system events), the Event reports provide additional features. The reports enable you to organize, export, and print the event data.

The *EMC NetWorker Avamar Integration Guide* provides information on Avamar.

Event reports can include this information:

- Number of events
- Priority of events
- Category of events
- Server name
- Server type
- Event time
- Notes and annotations

---

#### Note

When an event has been resolved, it does not remain in the records.

Types of event reports and configuration

---

The Events report category includes both basic and drill-down reports. The report's Configure tab allows you to limit the scope of the report.

The Event parameters are described in this table. The specific parameters available depend on which Event report is being configured.

---

#### Note

Data retention policies do not have any impact on Event reports.

---

**Table 66** Event parameters

| Configuration parameter | Description                                                                                                       | Options                                                                |
|-------------------------|-------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------|
| Server Name             | Selects one or more managed hosts.                                                                                | Selected server names                                                  |
| Server Type             | Selects some or all server types in the enterprise. Only the names of servers that have current events are shown. | Console<br>NetWorker<br>Avamar                                         |
| Priority                | Selects only priority events.<br>Priority represents the relative severity of the event.                          | Warning<br>Waiting<br>Notice<br>Info<br>Emergency<br>Critical<br>Alert |
| Category                | Selects only category events, or all categories. Category refers to the source of the event.                      | Database Backup<br>Registration<br>Savegroup                           |
| Event Time              | Selects a time range.<br>This parameter applies only to the Annotation Details report.                            | Event time (range)                                                     |

### Event basic reports

Within the Events report category, select any of the basic reports listed in the user interface. When a report has been chosen, the Configuration tab displays boxes listing the selected parameters for that report.

To exclude unwanted parameters from the report, remove them from the list. [Configuring a report on page 395](#) provides information about selecting and removing parameters.

### Additional information

These resources provide more information about the contents of Event reports:

- [Working with notes on page 426](#) provides information on NetWorker Console notes.
- The *EMC NetWorker Error Message Guide* provides descriptions of NetWorker software error messages and troubleshooting procedures.
- [Troubleshooting on page 675](#) provides information on troubleshooting NetWorker software issues.

### Event drill-down reports

The drill-down reports consist of multiple Event basic reports, connected in a predetermined sequence. [Drill-down reports on page 394](#) provides general information about drill-down reports.

The configuration parameters for a drill-down report are the same as the parameters for the top-level report in the report sequence. Thus, if the top layer of the drill-down report is a Server Summary report, the configuration parameters are the same as they would be for the basic report, Server Summary. When a report has been chosen, the Configuration tab displays boxes listing the selected parameters for the top-level report. To exclude

unwanted parameters from the report, remove them from the list. [Configuring a report on page 395](#) provides information on selecting and removing parameters.

## Host reports

The Hosts report category includes only basic reports. There are two basic reports, as described in this table.

**Table 67** Host reports

| Report name          | Purpose                                                                                                                                                                                                                                                                                                                            | Configuration parameters | Default                      |
|----------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------------|------------------------------|
| Host List            | <p>Provides an overview of servers in the enterprise, including:</p> <ul style="list-style-type: none"> <li>• Whether the Capture Events feature is enabled for the server.</li> <li>• Whether the Gather Report Data feature is enabled for the server.</li> <li>• Where the server is located in the enterprise path.</li> </ul> | None                     | All servers                  |
| Enterprise Inventory | <p>Allows movement through the Enterprise. Limit the report's scope by first viewing one of the lower-level folders within the Enterprise:</p> <ul style="list-style-type: none"> <li>• Start from Enterprise folder.</li> <li>• Start from selected folder.</li> </ul>                                                            | Enterprise Path          | Start from Enterprise folder |

[Enterprise on page 480](#) provides a description of the Enterprise and its folders.

## User reports

The Users report category provides information on NetWorker Console user activity. [NMC Server Management on page 467](#) provides information about NetWorker Console users and creating user accounts.

The Users report category includes only basic reports, no drill-down reports. The Full Name and Description information appears in the User reports only if this information was specified when the user was created.

## Device reports

Device reports provide information about the way devices are being used. They show scheduled and manual backup activity on one or more selected devices over time. You can identify periods of heavy activity or inactivity. Device reports aid NetWorker administrators in performance tuning, and they help identify bottlenecks. For example, if all drives are being used continuously for a long period of time, at maximum throughput, backup speeds may improve by adding tape drives or moving clients to another backup server.

### Types of Device reports and configuration

The Devices report category includes only one report, the Drive Utilization report. This report, which is a drill-down report, supports NetWorker servers running NetWorker software release 7.3 or later. The report includes backup activity data for all device types, including advanced file type devices and digital data storage devices.

When viewing a Drive Utilization report as a chart, it is automatically displayed as a Gantt chart, where the backup activity level of one or more devices is depicted in relation to time. Unlike with other reports, you cannot choose an alternate chart type.

Placing the cursor over the chart in Save Set view displays a tool tip that provides this information:

- Save set name
- Start time
- End time
- Client name
- Throughput value

Placing the cursor over the chart in Drive View displays a tool tip that provides this information:

- Drive
- Start time
- End time
- Throughput value

#### **Note**

One of the activities included in the Drive Utilization report is throughput. Since the Drive Utilization Report provides data for backup activities only, throughput values will normally be non-zero. However, zero (0) is considered a valid throughput value.

## Cloud backup and recover reports

Cloud backup and recover reports display information on the Cloud usage for scheduled backups and recovers that are performed by the NetWorker server to and from the Cloud storage device.

Types of Cloud backup and recover reports and configuration

The Cloud backup and recover reports category includes basic and drill-down reports. [Drill-down reports on page 394](#) provides general information about drill-down reports.

The Configure tab allows you to limit the scope of the report that was selected. The parameters available within the Cloud backup and recover report are described in this table. The specific parameters available depends on which Cloud backup and recover report is selected.

**Table 68** Cloud backup and recover parameters

| Parameter   | Description                                                                                                                                                                                        | Options               |
|-------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------|
| Server Name | Selects managed hosts within the enterprise.                                                                                                                                                       | Selected server names |
| Start Time  | Limits the report to a specified time range. The default range is one day for the Backup Details report.<br>The date/time format available depends on the language locale of the operating system. | start time (range)    |
| Device Name | Selects the devices used for backup and recover.                                                                                                                                                   | Selected device names |

## Cloud backup and recover reports

Within the Cloud backup and recover report category, choose any of the basic reports listed in the user interface. Once a report is chosen, the Configuration tab displays boxes with lists of the selected parameters for that report. To exclude unwanted parameters from the report, delete them from the list. [Configuring a report on page 395](#) provides information on selecting and removing parameters.

Cloud backup and recover reports can include this information:

- NetWorker server — Name of the server.
- Device name — Name of the device used for backup or recover.
- Device type — Type of the Cloud storage device, for example, Atmos.
- Login Account — Cloud username used for logging in.
- Size — Backup or Recover size.
- Compression ratio — Ratio of the bytes of information written to or read from the Cloud to the total size of the backup or recover.
- Bytes transferred — Total number of bytes written to or read from the Cloud.
- Start time — Start time for the backup or recover.
- End time — End time for the backup or recover.
- Save Set Name — Displayed only for backup.
- User name — Name of the user who initiated the recover. Displayed only for recover.
- Client name — Displays the name of the client that was backed up. In case of recover, source client name is displayed.
- Status — Displays the status of backup or recover. For example: succeeded, failed, and so on.

The Device Backup Summary and Device Recover Summary reports can be viewed in both Chart and Table modes. The other reports can be viewed in Table mode. [Interactive and document mode chart types on page 401](#) provides general information on charts.

## Inactive files

A NetWorker administrator can manage inactive files on a client or group and set the NetWorker software to automatically generate a list of inactive files in an environment. Inactive files are files that have not been accessed or modified other than being backed up regularly. The period of time a file has been inactive is called the Inactivity Threshold.

The inactivity files report is not supported on releases earlier than release 7.4 of the NetWorker servers.

Client support for this feature will be enabled only on Windows platforms.

The Inactive files report is a drill-down report that lists the inactive files from the latest scheduled backup. The report operates at both the client and group level.

The inactive files report can do the following:

- Generate a report on the percentage of inactive files backed up as part of a group.
- Set the threshold time periods per group so that the percentage of inactive files in that group does not exceed the threshold time period.
- Set alerts so that the NetWorker software sends an alert when the threshold set for a group is exceeded.
- Provide a report that details the percentage of inactive files backed up as part of a group.
- Report the percentage of inactive files per client.

The range limit specification given to configure File Inactivity Threshold and File Inactivity alert threshold attributes can be configured within the following ranges:

- File Inactivity Threshold attribute can be set between 0-365 days.
- File Inactivity Alert Threshold attribute can be set between 0-99.

## Group File Details

The Group file Details report provides statistical information about inactive files that are included in a scheduled backup. Data will be provided for every requested NetWorker group at the time of the last backup. Chart mode is the default mode for the report. The data can also be viewed in tabular mode for more detailed information.

When generating the Group Details report, you can specify the following parameters:

- One or more NetWorker servers. Only servers that have the Gather Reporting Data attribute turned on will appear in the selection list.
- One or more NetWorker groups for the selected NetWorker servers.

## Client File Details

The Client File Details report provides information about inactive files backed up for selected NetWorker clients. Data will be provided for every requested NetWorker client at the time of the last backup. Chart mode is the default mode for the report. The data can also be viewed in tabular mode for more detailed information.

When generating the Client File Details report, you can specify the following parameters:

- One or more NetWorker servers. Only servers that have the Gather Reporting Data attribute turned on will appear in the selection list.
- One or more NetWorker groups for the selected NetWorker servers.
- One or more NetWorker clients for the selected NetWorker servers.

## Customizing and saving reports

A customized report is a changed copy of a canned report. Canned reports can be changed and then saved under different names. You can preserve the report configuration parameters that are most useful for the enterprise.

A customized report can be rerun exactly the same way at a later time, and even by another user. This saves time if the same report information must be generated repeatedly.

Customized reports offer these additional options:

- Delete
- Rename
- Save
- Save As...
- Share

Since it is a copy, a customized report can be changed again and resaved, or even deleted. Reports can be saved either to preserve particular configurations (such as which servers are polled) or to save the view type (such as pie or bar chart).

---

**Note**

For NetWorker reporting purposes, the terms customized report and saved report are synonymous.

---

Customized reports appear alphabetically in the report hierarchy below the canned report from which they were created. They are stored in the Console database, which means that users can access them from wherever they are logged in to the NetWorker Console. This also makes them accessible by the command line reporting feature. [Command line reporting on page 421](#) provides more information about command line reporting.

These types of information are stored in customized reports:

- All options from the report's Configure tab
- Column display preferences for tables
- Orientation (portrait or landscape)
- Current view type (table or chart)

If the view type is Chart, then the current chart type (bar, pie, plot, or stacked bar) is also saved. For charts, the current chart axis selection is also saved. [Interactive and document mode chart types on page 401](#) provides more information about chart axis selection.

## Naming reports

When naming a report to save, keep in mind that the set of usable characters is limited in the same way as for hostnames and usernames. Report names may not contain:

- Characters having an ASCII representation number less than ASCII 32 (such as carriage return, bell, newline, escape)
  - Comma (,)
  - Slash (/) or backslash (\)
  - Double quote (“) or single quote (')
- 

**Note**

Report names are not case-sensitive. Also, canned reports cannot be deleted or customized, and then saved under the same name as a report that already exists under the same parent folder or directory.

---

## Saved file ownership and deleted users

When a user saves a report by using the Save As command, that user becomes the owner of the new report. When a Console Application Administrator deletes from the system a user who owns reports, then the Console Application Administrator sees a dialog box that shows all of the reports owned by that user, and can choose either to delete the reports or reset the owner to a different user.

## Sharing reports

By default, customized reports are stored as private for each user. This means that if a user saves a report, it appears only in that user's report hierarchy. A report's owner or the Console Application Administrator may, however, enable it for sharing.

Only the original owner of a customized report or the Console Application Administrator may select:

- Delete, to delete the report.

- Rename, to rename the report.
- Save, to resave the report.
- Share, to add sharing to, or remove sharing from, the report.
- If the Console Application Administrator removes sharing, the report becomes private again to the original owner, the report's creator.

Any user viewing a sharable report may perform these operations on the report:

- Change any runtime parameter of the report (such as configuration or view type).
- Run the report, but not save changes to the report.
- Copy the report by using the Save As command.
- Choose the Hide Other Users' Reports option to toggle the view of reports between only those owned by the user (both private and shared) and all shared custom reports.

If a user copies a sharable report with the Save As command, that user becomes the owner of the new report, which is initially set as not shared.

## Sharing a report

To enable sharing of a customized report:

### Procedure

1. From the **Console** window, click **Reports**.
2. Expand the report folder that contains the customized report to share.
3. Right-click the customized report, then select **Share**. The report is now shared, and is represented in the report hierarchy by a shared-report icon  or .

### Results

Once a report has been enabled for sharing, all users can see it in the report hierarchy.

---

### Note

The Share option is a toggle. To disable sharing, right-click the shared report and select **Share**.

---

## Exporting reports

Reports can be converted into other file formats and shared with others. The following table lists the file formats available when exporting reports.

**Table 69** Report export formats

| Format     | Purpose                                                                                |
|------------|----------------------------------------------------------------------------------------|
| PostScript | For printing.<br>Shows data totals.                                                    |
| PDF        | For printing or viewing with a PDF viewer such as Adobe Acrobat.<br>Shows data totals. |
| HTML       | For viewing in a browser.<br>Shows data totals.                                        |

**Table 69** Report export formats (continued)

| Format | Purpose                                                                                                                                                               |
|--------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| CSV    | For importing into other programs (such as spreadsheets) that accept the comma separated values (CSV) format.<br>Does not show data totals.<br>Use for raw data only. |

## Exporting a report

You can choose to export a report as a file in a different format (for example, HTML, PDF, CSV, or PostScript). To export a report to a different file format:

### Procedure

1. From the **Console** window, click **Reports**.
2. Expand the report folder that contains the report to export, then click the report.
3. Click the **View Report** tab to display the report.
4. Right-click the **View Report** tab, select **Export**, then select a format.

---

### Note

To sort or rearrange table columns in a report, export the report to CSV format. The columns then can be sorted or rearranged in a spreadsheet program.

5. In the **Save** dialog box, specify the filename and file location and then click **Save**.

## Exporting non-ASCII characters

Due to a limitation in the embedded reporting tool, reports that contain multibyte characters cannot be exported to PostScript or PDF formats. Such characters are replaced by a “?” character.

To obtain a printed version of such a report, print directly from the Console window, or export to HTML format.

---

### Note

ISO8859-1 characters can be exported to PostScript or PDF formats.

## Command line reporting

Command line reporting offers these features:

- Allows reports to be run offline, either as needed or by using scheduling software that makes reports available at predetermined times.
- Makes use of both canned and customized reports, which can be exported in various formats.
- Provides a more advanced feature that requires a fair amount of knowledge about running and scripting from the command prompt of the Console server. This feature should be reserved for advanced users.

---

#### Note

Command line reports may only be printed or run to generate exported output. They cannot be saved or shared. Drill-down reports cannot be run from the command line.

---

## The command line reporting program

The command line reporting program is `gstclreport`. It uses the JRE to run. Additionally, command line reports must be run on the NMC Console server host.

The options are typical command line options in the form of a hyphen (-) followed by one or two letters and an argument, if applicable. The *EMC NetWorker Command Reference Guide* or the UNIX man pages provide a complete description of the command and its options.

## System performance

Each time the `gstclreport` command is run, it starts a separate JVM, which can use many system resources. The `gstclreport` command runs a database query and generates report output by using the results. Since this uses both CPU and memory resources on the host computer, it could affect performance of NetWorker software and of the host. Consequently, depending on the system used, it is probably not wise to run more than a few instances of the `gstclreport` command at the same time.

## Security

The `gstclreport` command must contact the Console server in order to run a report. The command requires a valid username and password. A user either uses the -P option to type the password, or the command checks standard input to see whether the password is there. If a password is not supplied, the program prompts for a password.

On UNIX systems, use of the -P option is a security concern, because a user may type the `ps` command and see the commands that were used to start any program that is running.

To solve this problem, use scheduling software that can conceal password input. Alternatively, ensure that the scheduling system sends the password as standard input. For example:

```
echo password | gstclreport
```

A `cron` command can be used to schedule the report, or the command could be placed in a secure script file that is invoked by the `cron` command.

## Java runtime environment

Support of command line reporting requires JRE version 1.6 or later to run the `gstclreport` command. The JRE must be installed before installing NetWorker software.

Additionally, you must add an environment variable named `JAVA_HOME` to your NetWorker server host. Open either the `gstclreport.bat` or `gstclreport.sh` file and follow the instructions at the top of the file to set up the correct environment for command line reporting.

## Printing reports

All reports can be printed. This allows for the sharing of report data with users who are unable to view it online.

### Procedure

1. From the **Console** window, click **Reports**.
2. Expand the report folder that contains the report to print, then click the report.
3. Click the **View Report** tab to display the report.
4. Right-click anywhere on the **View Report** tab, then select **Print**.
5. From the **Print** dialog box, select the appropriate options on each tab, then click **Print**.

The -x print option in the `gstclreport` command is also available.

## Enterprise events monitoring

The NetWorker Management Console (NMC) provides the ability to view details of current NetWorker, Avamar, and Data Domain systems. Information that can be monitored includes activities and operations related to devices and libraries, and events that require user intervention. NMC makes the administration of servers more efficient by providing a centralized means of monitoring activity throughout an enterprise. [Managing various servers in the enterprise on page 481](#) provides details on adding hosts to be monitored.

## About Events

An event signals that user intervention is required. For example, if a NetWorker server needs a new tape, the server alerts users to the situation by posting an event to the Console window.

NetWorker software generates an event based on various factors, including the following scenarios:

- The software or hardware encounters an error that requires user intervention to resolve.
- A NetWorker savegroup has failed.
- Drive ordering or serial number mismatch issues — a description of the problem is provided, along with a corrective action to fix the problem.
- Capacity monitoring — for example, reaching the space threshold on the deduplication node.
- NetWorker software is unable to poll a host it is monitoring for events or for generating reports.
- A license or enabler code managed by the License Manager is about to expire.

Some situations do not result in the generation of an event. For example, when a license managed by the NetWorker Console (instead of by the License Manager) approaches its expiration date. In this situation, a message is recorded in the NetWorker logs, but an event is not generated until the expired license causes a backup to fail. Check the Administration window from time to time for important messages.

## Polling for System Events

From the System Options dialog box, you can set the poll interval for events and activities generated at system-level for the following:

- Events and reporting (in seconds)
- NetWorker activities (in seconds)
- Data Domain events (in seconds)
- NetWorker libraries (in hours)
- Avamar events (in hours)

---

### Note

Event polling for NetWorker libraries and Avamar events can only be done to a maximum of once per hour. [Setting system options to improve NMC server performance on page 470](#) provides information on setting polling intervals.

---

## Enabling or disabling the Capture Events option

The Capture Events option must be enabled for a given server before NetWorker software can monitor that server for events. This option is selected by default when a host is added.

### Procedure

1. From the **Console** window, click **Enterprise**.
2. Select the host for which the capturing of events is to be disabled or enabled.
3. Right-click the appropriate application, then select **Properties**.
4. Complete one of these steps as required:
  - To enable captured events, select **Features** > **Capture Events**.
  - To disable captured events, select **Features**, clear the **Capture Events** checkbox.  
For Avamar servers, the Capture Events option monitors only system-level events. The Avamar documentation provides other event information.
5. If the host is a Data Domain system, select the **Configure SNMP Monitoring** tab.
  - a. Enter **public** in the SNMP community string field.
  - b. Enter the value of the SNMP process port. The default port is **162**.
  - c. Select the **SNMP Traps** (Data Domain system events) to be monitored by NetWorker.
6. Click **OK**.

## Event viewing

To view events, from the Console window, click **Events**. If any events exist, they are displayed in the Console window.

The Console window includes columns that provide specific types of information about each event. The following table describes the various columns and the information they provide for NetWorker events.

**Table 70** Events columns

| Column      | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |
|-------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Priority    | Represents the relative severity of the problem by displaying one of seven icons.                                                                                                                                                                                                                                                                                                                                                                                                                    |
| Server Name | Identifies the host that caused the event to be generated.                                                                                                                                                                                                                                                                                                                                                                                                                                           |
| Server Type | Identifies the type of server to which the event belongs. Server types include but are not limited to NetWorker, Avamar, and Data Domain.                                                                                                                                                                                                                                                                                                                                                            |
| Time        | Indicates the day of the week and time that the Console server discovered the problem. The time which an event is reported is always based on the time zone of the Console server. For example: If a savegroup fails at 11:00 A.M. in New York, a Console server in Los Angeles reports the event for the savegroup as occurring at 8:00 A.M.<br>Note: The time format presented depends on the current locale setting. <a href="#">Date and time formats on page 396</a> provides more information. |
| Category    | Classifies the source of the problem.                                                                                                                                                                                                                                                                                                                                                                                                                                                                |
| Message     | Displays the text of the error message that generated the event.                                                                                                                                                                                                                                                                                                                                                                                                                                     |
| Annotation  | Displays an icon when an annotation has been made. An annotation is a log associated with an event. <a href="#">Working with annotations on page 426</a> provides more information.                                                                                                                                                                                                                                                                                                                  |
| Note        | Provides an editable field for making brief notes associated with an event. <a href="#">Working with notes on page 426</a> provides more information.                                                                                                                                                                                                                                                                                                                                                |

## Event priorities

Each event is designated one of seven possible priorities. The following table lists the event priorities and the information they provide. When the Console window sorts events by priority, it lists the events in alphabetical order, with Emergency between Critical and Information.

**Table 71** Event priorities

| Icon | Priority     | Description                                                                                                                         |
|------|--------------|-------------------------------------------------------------------------------------------------------------------------------------|
|      | Alert        | Error condition detected by the NetWorker server that should be fixed by a qualified operator.                                      |
|      | Critical     | Severe error condition that demands immediate attention.                                                                            |
|      | Emergency    | Condition exists that may cause NetWorker software to fail unless corrected immediately. This icon represents the highest priority. |
|      | Information  | Information about the current state of the server. This icon represents the lowest priority.                                        |
|      | Notification | Important information.                                                                                                              |
|      | Waiting      | Indication that the NetWorker server is waiting for an operator to perform a routine task, such as mounting a tape.                 |

**Table 71** Event priorities (continued)

| Icon                                                                              | Priority | Description                   |
|-----------------------------------------------------------------------------------|----------|-------------------------------|
|  | Warning  | Non-fatal error has occurred. |

## Working with notes

The Note column of the Console window provides a place to record brief administrative information about an event. For example, you can enter:

- Name of the NetWorker administrator or operator assigned to the event.
  - Letters or numbers that allow the sorting of events into a preferred order.
- A note can contain up to 30 characters, and can be edited or deleted.

### Adding a note

#### Procedure

1. From the **Console** window, click **Events**.
2. Double-click the cell of the **Note** column corresponding to the appropriate event, then type the text of the note in the cell.
3. After entering the text, click outside the cell.

### Editing a note

#### Procedure

1. From the **Console** window, click **Events**.
2. Double-click the note to edit, then change the text as appropriate.
3. After editing the note, click outside the cell.

### Deleting a note

#### Procedure

1. From the **Console** window, click **Events**.
2. Double-click the note, highlight the text in the cell, then press **Delete**.
3. After deleting the note, click outside the cell.

## Working with annotations

The Annotation column provides a place to record comments associated with an event, and can accommodate more information than the Note column. Each annotation can be up to 12 KB in size. For example, use annotations to log steps taken to resolve an event.

When an annotation has been added to an event, an icon appears in the Annotation column of the Events window. Multiple annotations can be added to a single event, and unlike notes, they cannot be edited or deleted.

### Viewing annotations

#### Procedure

1. From the **Console** window, click **Events**.

2. Right-click the event with the annotation to be viewed, then select **Annotation**. Annotations are listed in descending order, with the most recently added annotation at the top of the list.
3. After viewing the annotation, click **Cancel** to close the dialog box.

## Adding an annotation

### Procedure

1. From the **Console** window, click **Events**.
2. Right-click the event to be annotated, then select **Annotation**. The **Event Annotation** dialog box appears.
3. Type the text of the annotation.
4. To clear the text just entered, click **Reset**.
5. Click **OK**.

## Dismissing an event

After an event has been viewed and acted on, it can be dismissed from the Console window. This helps prevent other users from acting unnecessarily on events that have already been resolved.

---

### Note

Dismissing an event makes it disappear from the Console window for all NetWorker users.

---

### Procedure

1. From the **Console** window, click **Events**.
2. Right-click the event to dismiss, then select **Dismiss**.
3. Click **Yes** to confirm the dismissal.

### Results

There are slight differences in how event dismissals are handled, depending on the source:

- Events from NetWorker software are automatically dismissed in the Console window when the problem that triggered the event is resolved.
- Events from device ordering or serial mismatch issues are automatically dismissed in the Console window when the problem is resolved via the corrective action provided.

System events from an Avamar server (deduplication node) are not automatically dismissed in the Console window when the problem that triggered the event is solved. These events must be manually dismissed in the Console window.



# CHAPTER 16

## NetWorker server events reporting and monitoring

This chapter contains the following topics:

- [Monitoring NetWorker server activities](#)..... 430
- [Notifications](#)..... 445
- [Reporting group status and backup job status](#)..... 458
- [Reporting recover job status](#)..... 464

## Monitoring NetWorker server activities

Monitor the activities of an individual NetWorker server by using the NetWorker Administration application.

To access the NetWorker Administration application to monitor a NetWorker server:

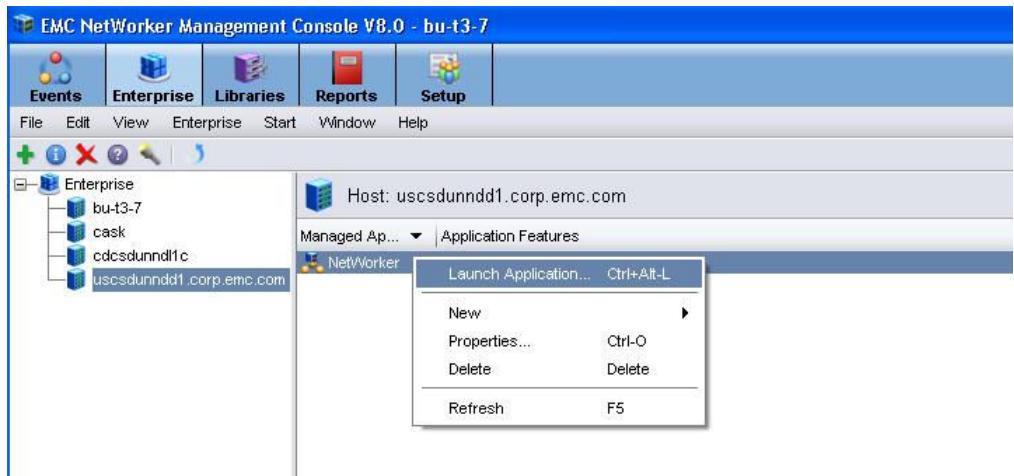
### Procedure

1. From the **NMC Console** window, click **Enterprise**.
2. In the **EMC NetWorker Management Console Enterprise** view, select the appropriate NetWorker server.
3. Highlight the host's Managed Application, then right-click and select **Launch Application**.

The **Administration** window appears.

The following figure shows how to select the NetWorker managed application.

**Figure 30** Selecting a NetWorker Managed Application



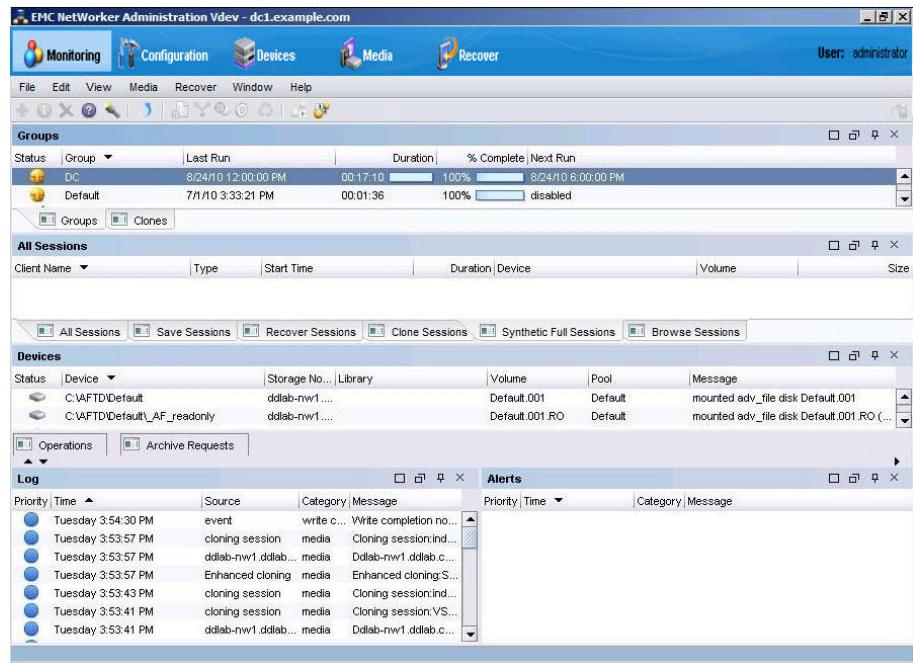
## About the Monitoring window

In the Administration window taskbar, select Monitoring to view the details of current NetWorker server activities and status, such as:

- Automatic and manual savegroups
- Archiving, cloning, recovering, synthetic backups, and browsing of client file indexes
- Alerts and log messages, and operations related to devices and jukeboxes

While the Monitoring window is used primarily to monitor NetWorker server activities, it can also be used to perform certain operations. These operations include starting, stopping, or restarting a group backup, as well as, starting and monitoring save set clones.

The following figure shows the Monitoring window.

**Figure 31** Monitoring window

The Monitoring window includes a docking panel that displays specific types of information. Select the types of information you want to view from the docking panel.

A portion of the Monitoring window, known as the task monitoring area, is always visible across all windows. A splitter separates the task monitoring area from the rest of the window. You can click and move the splitter to resize the task monitoring area. The arrow icon in the top-right corner of the Monitoring window allows you to select which tasks you want to appear in this view.

Smaller windows appear within the Monitoring window for each window. Each smaller window, once undocked, is a floating window and can be moved around the page to customize your view. You can select multiple types from the panel to create multiple floating windows that can be viewed at the same time. The following table describes the various types of information available in the docking panel and the details each one provides.

**Table 72** Monitoring window panel

| Window   | Information provided                                                                                                                                                                                                                                                                                                                                                                                            |
|----------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Groups   | Lists all groups related to the server, the backup status, the time the last backup was run, the duration of the backup, the completion percentage, and the next time the backup will run. <a href="#">Groups window on page 432</a> provides more information.                                                                                                                                                 |
| Clones   | Lists all scheduled clone jobs with the last start time, the last end time, and additional details on the included save sets. <a href="#">Clones window on page 434</a> provides more information.                                                                                                                                                                                                              |
| Sessions | Allows you to customize whether to display all session types, or only certain session types. The information provided depends on which session type you select. For example, if you select Save Sessions, the window lists clients, save sets, groups, backup level, backup start time, duration of the backup, devices, rate, and size. <a href="#">Sessions window on page 435</a> provides more information. |

**Table 72** Monitoring window panel (continued)

| Window           | Information provided                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |
|------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Alerts           | Lists the priority, category, time, and message of any alerts. <a href="#">Alerts window on page 436</a> provides more information.                                                                                                                                                                                                                                                                                                                                                                                                                                                         |
| Devices          | Lists devices, device status, storage nodes, libraries, volumes, pools, and related messages. <a href="#">Devices window on page 437</a> provides more information.                                                                                                                                                                                                                                                                                                                                                                                                                         |
| Operations       | Lists the status of all library and silo operations, including nsrjb operations run from the command prompt. Also lists user input, libraries, origin, operation data, operation start time, duration of the operation, progress messages, and error messages.<br>When displaying Show Details from the Operations window, the length of time that the window is displayed is controlled by the value entered in the Operation Lifespan attribute on the Timers tab of the Properties dialog box for the corresponding library. To access library properties, click Devices in the taskbar. |
| Log              | Lists messages generated by the NetWorker server, including the priority of each message, the time the message was generated, the source of the message, and the category. <a href="#">Log window on page 440</a> provides more information.                                                                                                                                                                                                                                                                                                                                                |
| Archive Requests | Lists the status of all Archive Requests configured on the server, including the last time the data was archived, the date and time of the next scheduled archive, and any annotations. <a href="#">Archive Requests window on page 440</a> provides more information.                                                                                                                                                                                                                                                                                                                      |

## Groups window

The Groups window displays groups that are in the process of completing, or have completed, their backup.

You can use this window to:

- Identify which groups backed up successfully.
- Identify which groups failed.
- Start, stop, or restart group backups.

The backup of a client group may fail for one of the following reasons:

- The NetWorker server failed.
- The NetWorker client failed.
- The network connection failed.

To find out more about a backup failure, check Group Backup details. [Viewing group backup details on page 434](#) provides more information.

## Groups window backup status

The backup status is represented by an icon. The following table lists and describes each of the icons.

**Table 73** Groups window icons

| Icon | Label        | Description                              |
|------|--------------|------------------------------------------|
|      | Being cloned | The group backup is being cloned.        |
|      | Failed       | The group backup failed.                 |
|      | Interrupted  | The group backup was interrupted.        |
|      | Never ran    | The group backup never ran.              |
|      | Running      | The group backup is running.             |
|      | Successful   | The group backup successfully completed. |
|      | Probing      | The group is in a probing state.         |

When items on the Groups window are sorted by the Status column, they are sorted in alphabetical order based on the label of the icon.

Consider the following when a group is in a probing state:

- A message is sent when the group starts and finishes the probe operation.
- The results of the probe operation (run backup/do not run backup) are also logged.
- Probes do not affect the final status of the group, and the group status does not indicate the results of the probe.
- If probing indicates that a backup should not run, then the group status reverts back to its state prior to the group running.
- Check the results of the probe in the Log window to ensure that the probe indicates that the backup can be taken.

## Groups backup operations

This section describes how to use the Monitoring window to start, stop, and restart group backups.

### Starting a group immediately

You can override the scheduled backup start time and start the group manually. This is equivalent to selecting Start Now in the Autostart attribute of the Group resource.

When a group backup is started manually, the NetWorker server runs the backup at the level of the next scheduled backup, such as full, levels 1 through 9, incremental, or consolidated.

#### Procedure

1. From the Administration window, click **Monitoring**.

2. Click **Groups** in the docking panel.
3. Right-click the group to start, then select **Start**.
4. Click **Yes** to confirm the start.

### Results

The NetWorker server immediately backs up the clients in the group.

### Stopping a group

#### Procedure

1. From the **Administration** window, click **Monitoring**.
2. Click **Groups** in the docking panel.
3. Right-click the group to stop, then select **Stop**.
4. Click **Yes** to confirm the stop.

### Restarting groups

The backup (including synthetic full backup) continues from the point at which it was stopped.

#### Procedure

1. From the **Administration** window, click **Monitoring**.
2. Click **Groups** in the docking panel.
3. Right-click the group to restart, then select **Restart Group**.
4. Click **Yes** to confirm the restart.

### Viewing group backup details

#### Procedure

1. From the **Administration** window, click **Monitoring**.
2. Click **Groups** in the docking panel.
3. Right-click the group to view, then select **Show Details**. The **Group Backup Details** dialog box appears.
4. View detailed information related to the group backups. If any messages were generated, the **Show Messages** button is enabled. Click **Show Messages** to view the messages.
5. Click **OK** to close the **Group Backup Details** dialog box.

## Clones window

The Clones window displays the scheduled clone jobs and their completion status. This window also identifies which client save sets are cloned successfully and which save sets are not cloned successfully. You can also use this window to start a scheduled clone job immediately.

### Scheduled clone operations

This section describes how to use the Monitoring window to start a scheduled clone operation and how to view the clone details for a client's save set.

## Starting a scheduled clone immediately

You can start a scheduled clone job at any time instead of waiting for the scheduled start time.

### Procedure

1. From the **Administration** window, click **Monitoring**.
2. Click **Clones** in the docking panel.
3. Right-click the scheduled clone to start, then select **Start**.
4. Click **Yes** to confirm the start.

### Results

The NetWorker server immediately starts the scheduled clone job.

## Viewing the save sets for a scheduled clone

You can view the NetWorker clients and their save sets that are included in a schedule clone job. You can also determine which save sets were cloned successfully and which ones were not.

### Procedure

1. From the **Administration** window, click **Monitoring**.
2. Click **Clones** in the docking panel.
3. Right-click the scheduled clone to view, then select **Show Details**. The **Clone Details** dialog box appears.
4. Click **OK** to close the **Clone Details** dialog box.

## Sessions window

Use the Sessions window to view the sessions that are running on a NetWorker server. You can change the view of this window to display these sessions:

- Save
- Recover
- Clone
- Browse
- Synthetic Full/Rehydrated Sessions
- All

The default setting for the Sessions window is to display save sessions. [Changing displayed session types on page 435](#) provides instructions on viewing other session types.

## Changing displayed session types

The column headings displayed on this window will differ depending on the type of sessions you chose to display.

### Procedure

1. From the **Administration** window, click **Monitoring**.
2. Click **Sessions** in the docking panel.

3. Go to **View >> Show** and select the type of sessions to display. To display all sessions currently running on the NetWorker Server, regardless of type, select **All Sessions**.

## Stopping a session

You can stop a session (backup, synthetic full backup, clone, and recovery sessions) from the Monitoring window, even if the session was started by running savegrp.

To stop a session, right-click the session in the window and select Stop from the drop-down.

The following table provides a list of actions that can be stopped from NMC.

**Table 74** Sessions that can be stopped from NMC

| Session type                             | Stop from NMC? |
|------------------------------------------|----------------|
| Save by Save Group                       | Yes            |
| Synthetic Full by Save Group             | Yes            |
| Clone by Save Group                      | Yes            |
| Schedule Clone                           | Yes            |
| Manual Save                              | No             |
| Manual Clone via NMC                     | No             |
| Manual Clone via CLI                     | No             |
| Winworker and CLI Recovery               | No             |
| Recovery started from Recover wizard     | Yes            |
| VMware Backup Appliance Save and Recover | No             |

### NOTICE

When a session is cancelled from NMC, this does not impact any other group operations running.

## Alerts window

The Alerts window displays alerts generated by a particular NetWorker server or Data Domain system that has devices configured on the NetWorker server. It includes priority, category, time, and message information.

The alert priority is represented by an icon. The following table lists and describes each of the icons.

**Table 75** Alerts window icons

| Icon | Label    | Description                                                                                    |
|------|----------|------------------------------------------------------------------------------------------------|
|      | Alert    | Error condition detected by the NetWorker server that should be fixed by a qualified operator. |
|      | Critical | Severe error condition that demands immediate attention.                                       |

**Table 75** Alerts window icons (continued)

| Icon | Label        | Description                                                                                                                           |
|------|--------------|---------------------------------------------------------------------------------------------------------------------------------------|
|      | Emergency    | Condition exists that could cause NetWorker software to fail unless corrected immediately. This icon represents the highest priority. |
|      | Information  | Information about the current state of the server. This icon represents the lowest priority.                                          |
|      | Notification | Important information.                                                                                                                |
|      | Waiting      | The NetWorker server is waiting for an operator to perform a task, such as mounting a tape.                                           |
|      | Warning      | Non-fatal error has occurred.                                                                                                         |

When items on the Alerts window are sorted by the Priority column, they are sorted in alphabetical order based on the label of the icon.

## Removing alerts

Individual messages can be deleted from the Alerts and Events tables by removing them from the Events table. The two views show the same messages. To delete a message in the Events table, right-click the message and select Dismiss.

## Devices window

The Devices window allows you to monitor the status of all devices, including NDMP devices. If the NetWorker server uses shared and logical devices, the window is adjusted dynamically to present a set of columns appropriate for the current configuration.

If the current server configuration includes a shared device, a Shared Device Name column appears on the Devices window. The name of the shared device appears in the Shared Device Name column. If other devices for that configuration are not shared devices, then the Shared Device Name column is blank for those devices. Additionally, since only a single device per hardware ID can be active at any given moment, the information for inactive shared devices is filtered out, so only one device per hardware ID is presented on the window at any time.

If the current server uses an AlphaStor library, then a Logical Name column is added to the Devices window to accommodate logical devices.

The device status is represented by an icon. The following table lists and describes each of the icons.

**Table 76** Devices window icons

| Icon | Label                   | Description                     |
|------|-------------------------|---------------------------------|
|      | Library device active   | The library device is active.   |
|      | Library device disabled | The library device is disabled. |
|      | Library device idle     | The library device is idle.     |

**Table 76** Devices window icons (continued)

| Icon                                                                              | Label                       | Description                         |
|-----------------------------------------------------------------------------------|-----------------------------|-------------------------------------|
|  | Stand-alone device active   | The stand-alone device is active.   |
|  | Stand-alone device disabled | The stand-alone device is disabled. |
|  | Stand-alone device idle     | The stand-alone device is idle.     |

When items on the Devices window are sorted by the Status column, they are sorted in alphabetical order based on the label of the icon.

## Operations window

The Operations window displays information about device operations. It includes this information:

- Status of the operation.
- Name of the library.
- Whether or not the operation requires user input.  
For example, a labeling operation may want the user to acknowledge whether the system should overwrite the label on a tape. [Entering user input on page 439](#) provides instructions on how to deal with a user input notification.
- The origin, or source, of the operation.  
For example, the interface, nsrb or the NetWorker server.
- Time the operation started.
- Type of operation.
- Duration of the operation.
- Status messages from the operation.
- Any error messages.

**NOTICE**

Only the last error message of the operation will appear in the Error Messages column. Move the mouse pointer over the cell containing the last error message to display the entire list of error messages.

---

The operation status is represented by an icon. The following table lists and describes each of the icons.

**Table 77** Operations window icons

| Icon                                                                                | Label  | Description                                          |
|-------------------------------------------------------------------------------------|--------|------------------------------------------------------|
|  | Failed | The operation failed.                                |
|  | Queued | The operation is waiting in the queue to run.        |
|  | Retry  | The operation failed, but may work if you try again. |

**Table 77** Operations window icons (continued)

| Icon | Label      | Description                           |
|------|------------|---------------------------------------|
|      | Running    | The operation is running.             |
|      | Successful | The operation completed successfully. |
|      | User Input | The operation requires user input.    |

When items on the Operations window are sorted by the Status column, they are sorted in alphabetical order based on the label of the icon.

## Viewing operation details

The Operation Details dialog box opens, providing information about the completion of the operation. The Completion Time displays the time the operation finished. The time it took to complete the operation is the difference between the completion and start times of the operation.

To save operation details to a file, click Save in the Operation Details dialog box. When prompted, identify a name and location for the file.

### Procedure

- From the **Administration** window, click **Monitoring**.
- Click **Operations** in the docking panel.
- Right-click the appropriate operation, then select **Show Details**.

## Stopping an operation

Certain operations can be stopped from the Operations window.

### Procedure

- From the **Administration** window, click **Monitoring**.
- Click **Operations** in the docking panel.
- Right-click the operation to stop, then select **Stop**.
- Click **Yes** to confirm the stop.

#### NOTICE

Operations that were started from a command line program such as the nsrjb command, cannot be stopped from the Operations window. To stop these operations, press Ctrl-c from the window where the command was started.

## Entering user input

If the system requires user input, select the labeling operation in slow/verbose mode and the Supply User Input icon appears.

### Procedure

- Right-click the operation, then select **Supply Input**.
- Confirm whether or not to supply input.
  - If **Yes**, and input is supplied, the icon in the User Input column disappears.

- If two users attempt to respond to the same user input prompt, the input of the first user will take precedence, and the second user will receive an error message.
- If No, and input is not supplied, the operation will time out and fail.

## Log window

To view the most recent notification logs, click the Log window from the docking panel in the Monitoring window. The Log window provides the priority, time, source, category, and message for each log.

**NOTICE**

If a particular log file is no longer available, check the log file on the NetWorker server. The log files are located in this directory:<NetWorker\_install\_path\logs. [Viewing log files on page 677](#) provides information about viewing log files.

The log priority is represented by an icon. The following table lists and describes each of the icons.

**Table 78** Log window icons

| Icon | Label        | Description                                                                                                                           |
|------|--------------|---------------------------------------------------------------------------------------------------------------------------------------|
|      | Alert        | Error condition detected by the NetWorker server that should be fixed by a qualified operator.                                        |
|      | Critical     | Severe error condition that demands immediate attention.                                                                              |
|      | Emergency    | Condition exists that could cause NetWorker software to fail unless corrected immediately. This icon represents the highest priority. |
|      | Information  | Information about the current state of the server. This icon represents the lowest priority.                                          |
|      | Notification | Important information.                                                                                                                |
|      | Waiting      | The NetWorker server is waiting for an operator to perform a task, such as mounting a tape.                                           |
|      | Warning      | Non-fatal error has occurred.                                                                                                         |

When items on the Log window are sorted by the Priority column, they are sorted in alphabetical order based on the label of the icon.

## Archive Requests window

The Archive Requests window displays the current status of all archive requests that are scheduled on the NetWorker server. Use this window to identify which archive requests are running, completed, or failed, as well as when they were last run, and when they are scheduled to run next.

The archive status is represented by an icon. The following table lists and describes each of the icons.

**Table 79** Archive requests window icons

| Icon | Label      | Description                         |
|------|------------|-------------------------------------|
|      | Disabled   | The scheduled archive is disabled.  |
|      | Failed     | The archive failed.                 |
|      | Running    | The archive is running.             |
|      | Scheduled  | The archive is scheduled to run.    |
|      | Successful | The archive completed successfully. |

When items on the Archive Requests window are sorted by the Status column, they are sorted in alphabetical order based on the label of the icon.

## Viewing details of an archive operation

From the Monitoring window, you can view the details of an archive request, including the start time, the most recent completion time, and other information such as the pool and clone pool to which the archive request will write its data.

### Procedure

1. From the Administration window, click **Monitoring**.
2. Click **Archive Requests** in the docking panel.
3. Right-click the appropriate archive request, then select **Show Details**.

The Archive Request Details dialog box opens, providing information about the completion of the archive request. The Completion Time displays the time the archive finished. The time it took to complete the archive is the difference between the completion and start times of the archive.

To save archive request information to a file, click **Save** in the Archive Request Details dialog box. When prompted, identify a name and location for the file.

## Archive request operations

Use the Monitoring window to perform a number of archive request operations, such as canceling manual clone jobs, or starting, stopping, restarting, and disabling archive requests. The Monitoring window can also be used to schedule archive requests to start at a specific time in the future. These operations are equivalent to changing the Status attribute of the Archive Request resource, described in [Scheduling data archives on page 311](#).

### Starting an archive immediately

You can start an archive immediately from within the Monitoring window. This will override and disable any scheduled archive for the selected archive request.

### Procedure

1. From the Administration window, click **Monitoring**.
2. Click **Archive Request** in the docking panel.
3. Right-click the appropriate archive request, then select **Start**.

4. Click **Yes** to confirm the start.

## Stopping an archive in progress

### Procedure

1. From the **Administration** window, click **Monitoring**.
2. Click **Archive Request** in the docking panel.
3. Right-click the appropriate archive request, then select **Stop**.
4. Click **Yes** to confirm the stop.

## Scheduling an archive to start automatically

You can also use the Monitoring window to schedule an archive to start automatically at a later time.

### Procedure

1. From the **Administration** window, click **Monitoring**.
2. Click **Archive Request** in the docking panel.
3. Right-click the appropriate archive request and select **Schedule Archive**.
4. In the **Schedule Archive Request** dialog box, type the time that the archive should start, by using the hh:mm format.
5. Click **OK**. The **Next Run** column on the **Archive Requests** window displays the entered time.

## Disabling a scheduled archive

If an archive request has a scheduled start time, you can disable the scheduled archiving.

### Procedure

1. From the **Administration** window, click **Monitoring**.
2. Click **Archive Requests** in the docking panel.
3. Right-click the appropriate archive request, then select **Disable Archive**.
4. Click **Yes** to confirm the disable.

## Recover window

The Recover window displays information about recover configurations created with the NMC Recovery Wizard.

You can use this window to:

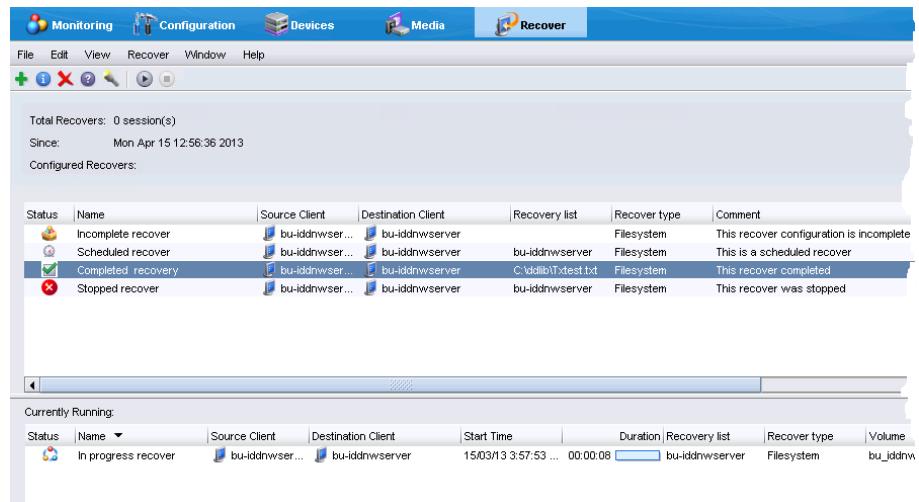
- Start the NMC Recovery Wizard to create new recover configurations or modify saved recover configurations.
- Identify the status of a recover configuration created with the NMC Recovery Wizard.
- Start and stop a recover job.

The Recover window is divided into five sections:

- Toolbar
- Summary
- Configured Recovers
- Currently Running

A splitter separates the Configured Recovers section from Currently running area. You can click and move the splitter to resize these two windows. The following table shows and example of the Recover window.

**Figure 32** Recovery Window



## Recover toolbar

The Recover toolbar provides you with the ability to quickly perform common recover operations. The following table summarizes the function of each toolbar button.

**Table 80** Recovery toolbar options

| Button | Function                                                                                                                                                                 |
|--------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|        | Starts the NMC Recover wizard to create a new recover configuration.                                                                                                     |
|        | Displays the properties window for the saved recover configuration selected in the Configured Recover window.                                                            |
|        | Displays the Find window at the bottom of the Recover window.                                                                                                            |
|        | Deletes the saved recover configuration selected in the Configured Recover window.                                                                                       |
|        | Displays online help for the Recover window.                                                                                                                             |
|        | Start the recover operation for a selected saved recover configuration. This option is only available for a recover configuration that has a Never run or Failed status. |
|        | Stop the in progress recover operation that you selected in the Currently Running window.                                                                                |

## Recover Summary

The Recover Summary section displays a high-level overview of recover jobs. This section includes the following information:

- Total Recovers: The total number of successful recover jobs.
- Since: The number of successful recover jobs since this date.

## Configured Recovers

The Configured Recovers window displays a list of saved recover configurations in a tabular format. You can sort the information by column. The Configured Recovers table displays the following information for each saved recover configuration:

- Status—The job status of a saved recover configuration
- Name
- Source client
- Destination client
- Recovery list
- Recover type—for example, filesystem or BBB
- Comment
- OS—the operating system of the source host
- Recover requestor—the Windows or UNIX account used to create the recover configuration.
- Start Time
- End Time
- Start date

**Table 81** Save recover configuration job status

| Icon | Description                                        |
|------|----------------------------------------------------|
|      | The last recover attempt failed.                   |
|      | The last recover attempt completed successfully    |
|      | The recover job has never run.                     |
|      | The recover job is scheduled to run in the future. |
|      | The recover job has expired.                       |

## Currently running

The Currently Running window displays a list of in progress recover jobs in a tabular format. You can sort the information by column. The Currently Running table displays the following information for each job:

- Status
- Name

- Source client
- Destination client
- Recovery list
- Recover type—for example, filesystem or BBB
- Volume
- Comment
- Device
- Size
- Total size
- % complete
- Rate (KB/s)
- Start time
- Duration
- Currently running

## Find

The Find section appears along the bottom of the Recover window, after you select the Find button on the Recover toolbar. Find allows you to search for keywords in the Configured Recovers window. The following table summarizes the available find options.

**Table 82** Find options

| Find option   | Description                                                                                                                                  |
|---------------|----------------------------------------------------------------------------------------------------------------------------------------------|
| Find          | Highlight the first saved recover configuration that contains the specified keyword.                                                         |
| Prev          | Highlight the previous saved recover configuration that contains the specified keyword.                                                      |
| Highlight All | Highlights each saved recover configuration that contains the specified keyword.                                                             |
| Sort Selected | Sorts each highlighted recover configuration in the Configured Recover table so that they appear at the top of the Configured Recover table. |
| Match case    | Make the keyword search case sensitive.                                                                                                      |

## Notifications

A notification provides information about events that occur in a NetWorker environment. You can configure the events to be reported and how the NetWorker server reports them to you. Specific programs can be executed when an event occurs, including third-party programs. By default, the NetWorker server sends notifications to log files that are located in the `NetWorker_install_dir\logs` directory on Windows and the `/nsr/logs` directory on UNIX.

The following sections provides information to manage event notifications:

- [Preconfigured notifications on page 446](#)
- [Customizing notifications on page 450](#)
- [Logging event notifications on page 455](#)

- [Creating a custom notification on page 456](#)
- [Editing a notification on page 456](#)
- [Copying a notification on page 456](#)
- [Deleting a custom notification on page 457](#)
- [Configuring owner notifications on page 457](#)
- [Savegroup completion and failure notifications on page 458](#)

## Preconfigured notifications

NetWorker is preconfigured to provide most of the event notifications required to monitor NetWorker events. The following table lists these preconfigured notifications and the associated actions performed by the NetWorker server.

**Table 83** Preconfigured notifications

| Notification                | Default action                                                                                                                                                                                                                                                                                                                                                                                                                                                                              |
|-----------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Bootstrap                   | Windows: Provides the syntax for the smptmail command to send an email to the administrators with the results of the bootstrap backup. The action attribute must be modified to replace mailserver with the actual hostname of the mail server. <a href="#">Using smptmail to email notifications on page 454</a> describes how to customize the smptmail command.<br>UNIX: Sends an email to the root account with the results of the bootstrap backup.                                    |
| Bootstrap backup failure    | Windows: Provides the syntax for the smptmail command to send an email to the administrator account stating that the bootstrap backup has failed. The action attribute must be modified to replace mailserver with the actual hostname of the mail server. <a href="#">Using smptmail to email notifications on page 454</a> describes how to customize the smptmail command.<br>UNIX: Sends an email to the root account with the results of a failed bootstrap backup.                    |
| Bus/Device Reset            | Windows: Provides the syntax for the smptmail command to send an email to the administrator account stating that the a bus or device reset has been detected. The action attribute must be modified to replace mailserver with the actual hostname of the mail server. <a href="#">Using smptmail to email notifications on page 454</a> describes how to customize the smptmail command.<br>UNIX: Sends an email to the root account stating that a bus or device reset has been detected. |
| Cleaning cartridge expired  | Windows: Reports to the <code>&lt;NetWorker_install_path&gt;\nsr\logs\media.log</code> file that a cleaning cartridge has expired.<br>UNIX: Sends an email to the root account stating that an expired cleaning cartridge has been detected.                                                                                                                                                                                                                                                |
| Cleaning cartridge required | Windows: Reports to the <code>&lt;NetWorker_install_path&gt;\nsr\logs\media.log</code> file that a device cleaning is required.<br>UNIX: Sends an email to the root account stating that an cleaning cartridge is required.                                                                                                                                                                                                                                                                 |
| Client install              | Windows: Reports the hostname and NetWorker client software version information to the <code>&lt;NetWorker_install_path&gt;\nsr\logs\media.log</code> file.                                                                                                                                                                                                                                                                                                                                 |

**Table 83** Preconfigured notifications (continued)

| Notification                                 | Default action                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |
|----------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|                                              | UNIX: Sends an email to root account: host host_name installed product_version.<br>Where host_name is the name of the NetWorker host, and product_version is the NetWorker client software release and build number.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     |
| Device cleaned                               | Windows: Reports that a device has been cleaned to the <NetWorker_install_path>\nsr\logs\media.log file.<br>UNIX: Sends an email to the root account stating that a device cleaning operation is complete.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |
| Device cleaning required                     | Windows: Reports that a device requires cleaning to the <NetWorker_install_path>\nsr\logs\media.log file.<br>UNIX: Sends an email to the root account stating that a device requires cleaning.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |
| Device disabled                              | Windows: Reports that a device has been automatically disabled to the <NetWorker_install_path>\nsr\logs\media.log file.<br>UNIX: Sends an email to the root account stating that a device has been automatically disabled.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |
| Device ordering issue detect                 | Windows: Provides the syntax for the smptmail command to send an email to the administrator account with the message “Check system device ordering. Moving device on NetWorker_server to service mode. To correct, scan for devices in NMC and re-enable the device. Refer to the section “Devices -> Replace a drive” in NetWorker Procedure Generator for full details. The action attribute must be modified to replace mailserver with the actual hostname of the mail server. <a href="#">Using smptmail to email notifications on page 454</a> describes how to customize the smptmail command.<br>UNIX: Sends an email to the root account with the message “Check system device ordering. Moving device on NetWorker_server to service mode. To correct, scan for devices in NMC and re-enable the device. Refer to the section “Devices -> Replace a drive” in NetWorker Procedure Generator for full details.” |
| Event log (Windows only)                     | Logs notification events triggered by events and priorities to the Event Log.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |
| Filesystem full - recovering adv_file space  | Launches the nsrim program to remove aborted and expired save sets. Used with advanced file type devices only.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |
| Filesystem full - waiting for adv_file space | Windows: Reports that the advanced file volume is full to the C:\Program Files \EMC NetWorker\logs\media.log file.<br>UNIX: Sends an email to the root account stating that an advanced file volume is full.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             |
| Inactive Files Alert                         | Windows: Reports that the space occupied by inactive files exceeds configured threshold to the C:\Program Files\EMC NetWorker\logs\messages log file.<br>Unix: Sends an email to the root account stating that the space occupied by inactive files exceeds configured threshold.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |

**Table 83** Preconfigured notifications (continued)

| Notification                  | Default action                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |
|-------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Index size                    | Windows: Reports a message that the size of the index will soon exceed the space available to the C:\Program Files\EMC NetWorker\logs\index.log file.<br>UNIX: Sends this email to root: "Check the size of the client file index because it will soon exceed the space available."                                                                                                                                                                                                                                                          |
| Log default                   | Windows: Sends data about NetWorker events to the C:\Program Files\EMC NetWorker\logs\messages log file.<br>UNIX: Directs data about the NetWorker events to logger. The logger utility sends the event with a tag of daemon.notice to the Operating system log file defined in the system log configuration file, for example syslog.conf.                                                                                                                                                                                                  |
| NetWorker Daemons Not Running | Windows: Provides the syntax for the smptmail program to send an email to the administrator account stating that NetWorker daemons are not running on the NetWorker server. The action attribute must be modified to replace mailserver with the actual hostname of the mail server. <a href="#">Using smptmail to email notifications on page 454</a> describes how to customize the smptmail program.<br>UNIX: Sends an email to the root account stating that NetWorker daemons are not running on the NetWorker server.                  |
| New Virtual Machine           | Windows: Reports a message that new virtual machines have been detected to the <NetWorker_install_path>\nsr\logs\messages log file.<br>UNIX: Sends an email to the root account stating that new virtual machines have been detected.                                                                                                                                                                                                                                                                                                        |
| Policy completion             | Windows: Sends an event notification to the <NetWorker_install_path>\nsr\logs\policy.log file with a message that a VMware protection policy has been completed.<br>UNIX: Sends an email to the root account with a message that a VMware protection policy has been completed.                                                                                                                                                                                                                                                              |
| Registration                  | Windows: Sends messages about the registration status of your NetWorker products to the <NetWorker_install_path>\nsr\logs\messages log file.<br>UNIX: Sends this email to root: check the registration status.                                                                                                                                                                                                                                                                                                                               |
| Resource File Corruption      | Windows: Provides the syntax for the smptmail program to send an email to the administrator account stating that resource file corruption has been detected on the NetWorker server. The action attribute must be modified to replace mailserver with the actual hostname of the mail server. <a href="#">Using smptmail to email notifications on page 454</a> describes how to customize the smptmail program.<br>UNIX: Sends an email to the root account stating that resource file corruption has been detected on the NetWorker server |
| Savegroup completion          | Windows: Reports the degree of success in completing all of the scheduled backups, cloning, and archive operations for a group to the <NetWorker_install_path>\nsr\logs\savegrp.log file.<br>UNIX: Sends an email to the root account of the NetWorker server to report the degree of success in completing all of the scheduled backups, cloning, and archive operations for a group.                                                                                                                                                       |

**Table 83** Preconfigured notifications (continued)

| Notification               | Default action                                                                                                                                                                                                                                                                                                                                                                                                                                                |
|----------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Savegroup failure          | Windows: Reports when a group backup fails to start at the scheduled time in the <NetWorker_install_path>\nsr\logs\savegrp.log file.<br>UNIX: Sends an email to root to report when a group backup fails to start at the scheduled time.<br><br>Possible reasons include that the previously scheduled backup is still running.                                                                                                                               |
| Save set marked suspect    | Windows: Provides the syntax for the smptmail program to send an email to the administrator account when a save set has been marked suspect. The action attribute must be modified to replace mailserver with the actual hostname of the mail server. <a href="#">Using smptmail to email notifications on page 454</a> describes how to customize the smptmail program.<br>UNIX: Sends an email to the root account when a save set has been marked suspect. |
| Scheduled clone completion | Windows: Sends an event notification to the <NetWorker_install_path>\nsr\logs\clone.log file with a message that a scheduled clone operation has completed.<br>UNIX: Sends an email to the root account with a message that a scheduled clone operation has completed.                                                                                                                                                                                        |
| Scheduled clone failure    | Windows: Sends an event notification to the <NetWorker_install_path>\nsr\logs\clone.log file with a message that a scheduled clone operation has failed.<br>UNIX: Sends an email to the root account with a message that a scheduled clone operation has failed.                                                                                                                                                                                              |
| SNMP notification request  | Sends event notifications to a network management console. This notification occurs when the NetWorker SNMP module has been purchased and enabled. <a href="#">Configuring NetWorker SNMP notifications on page 598</a> provides details on SNMP notifications                                                                                                                                                                                                |
| Tape mount request 1       | Windows: Requests media be mounted in a device and displays a pending message in the <NetWorker_install_path>\nsr\logs\messages log file.<br>UNIX: Sends a request message to the system logger to mount a backup volume, using a local0 facility and an alert level.                                                                                                                                                                                         |
| Tape mount request 2       | Windows: Requests media be mounted in a device and displays a critical message.<br>UNIX: Sends a request message to the system logger to mount a backup volume, using a local0 facility and an alert level.                                                                                                                                                                                                                                                   |
| Tape mount request 3       | Windows: Sends a request to mount a backup volume with a priority of Alert, to the <NetWorker_install_path>\nsr\logs\media.log file.<br>UNIX: Sends an email to the root account requesting that the tape be mounted.                                                                                                                                                                                                                                         |
| Tape mount request 4       | Windows: Provides the syntax for the smptmail program to send an email to the administrator account that a Tape mount request 4 event has occurred. The action attribute must be modified to replace mailserver with the actual hostname of the mail server. <a href="#">Using smptmail to email notifications on page 454</a> describes how to customize the smptmail program.                                                                               |

**Table 83** Preconfigured notifications (continued)

| Notification                     | Default action                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   |
|----------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|                                  | UNIX: Sends an email to the root account stating that a Tape mount request 4 event has occurred.                                                                                                                                                                                                                                                                                                                                                                                                                 |
| Verify Label failed on unload    | Windows: Provides the syntax for the smptmail program, to send an email to the administrator account stating that a label verification on unload operation has failed. The action attribute must be modified to replace mailserver with the actual hostname of the mail server. <a href="#">Using smtpmail to email notifications on page 454</a> describes how to customize the smptmail program.<br>UNIX: Sends an email to the root account stating that a label verification on unload operation has failed. |
| VMware Protection Policy Failure | Windows: Sends an event notification to the <NetWorker_install_path>\nsr\logs\policy.log file with a message that a VMware protection policy failed.<br>UNIX: Sends an email to the root account with a message that a VMware protection policy failed.                                                                                                                                                                                                                                                          |
| Volume Marked full               | Windows: Provides the syntax for the smptmail program to send an email to the administrator account stating that a volume has been marked full. The action attribute must be modified to replace mailserver with the actual hostname of the mail server. <a href="#">Using smtpmail to email notifications on page 454</a> describes how to customize the smptmail program.<br>UNIX: Sends an email to the root account stating that a volume has been marked full                                               |
| Volume Scan needed               | Windows: Sends an event notification to the <NetWorker_install_path>\nsr\logs\media.log file with a message that a volume with the Scan needed flag is detected.<br>UNIX: Sends an email to the root account with a message that a volume with the Scan needed flag is detected.                                                                                                                                                                                                                                 |

## Customizing notifications

Notifications require the following three elements:

- [Events on page 450](#)
- [Actions on page 452](#)
- [Priorities on page 455](#)

## Events

Events are the activities on the NetWorker server that can trigger a notification.

The following table lists the events that trigger a notification.

**Table 84** Events

| Event     | Description                                                  |
|-----------|--------------------------------------------------------------|
| adv_file  | The file system is full and is waiting for additional space. |
| Bootstrap | The bootstrap backup failed.                                 |

**Table 84** Events (continued)

| Event                           | Description                                                                                |
|---------------------------------|--------------------------------------------------------------------------------------------|
| Bus/Device Reset                | A SCSI bus or device reset has occurred.                                                   |
| Cleaning cartridge expired      | A cleaning cartridge has expired and needs replacing.                                      |
| Cleaning cartridge required     | Mount the cleaning cartridge.                                                              |
| Client                          | NetWorker client software has been installed on a host.                                    |
| Deleted media                   | A media device has been deleted.                                                           |
| Device cleaned                  | A device has been cleaned.                                                                 |
| Device cleaning required        | A device requires cleaning.                                                                |
| Device disabled                 | A device has been automatically disabled.                                                  |
| Hypervisor                      | New virtual clients have been auto-discovered, or auto-discovery failed.                   |
| Index                           | An index needs attention.                                                                  |
| License expiration              | A license has expired.                                                                     |
| Media                           | A media related event occurred. For example, a volume may require mounting.                |
| Media attention                 | Media needs operator attention to mount or unmount backup volumes.                         |
| Media capacity                  | A volume has almost reached the maximum number of save sets allowed in the media database. |
| Media request                   | Media needs operator attention to mount backup volumes.                                    |
| Potential device ordering issue | A device ordering or serial mismatch error has occurred.                                   |
| Resource File                   | A resource file corruption has occurred                                                    |
| Registration                    | Product registration needs attention.                                                      |
| Savegroup                       | A backup group has completed the backup.                                                   |
| Savegroup failure               | A backup group has completed with failures.                                                |
| Server                          | Other server events (for example, restarting the NetWorker server).                        |
| Storage node                    | A storage node has been installed.                                                         |
| Volume scan needed              | A volume with the scan needed flag has been detected                                       |
| Write completion                | A write operation is complete.                                                             |

## Actions

The Actions attribute defines the action that the NetWorker server takes after an event notification occurs. The following table provides a summary of actions.

**Table 85** Actions

| Action   | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |
|----------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| eventlog | Windows only, logs the notification message to the event log. Priority determines whether the notification is an error, warning, or information-only message.                                                                                                                                                                                                                                                                                                                                                                                                             |
| nsrlog   | Windows only, sends a message about an event to a file. Use option f to identify a specific file. For example:<br>nsrlog -f log file path<br><br>If no option is specified, then messages go to the /nsr/logs/messages file.                                                                                                                                                                                                                                                                                                                                              |
| nsrlpr   | Windows only, prints information to a printer. Use option P to identify a specific printer. For example:<br>nsrlpr -P printer_name<br><br>The printer can also be a remote print server such as LAN manager printer. In this case, use the following syntax<br><br>nsrlpr -P \\server_name\printer_name<br><br><a href="#">Using nsrlpr to print notifications on page 453</a> provides more information about nsrlpr.                                                                                                                                                    |
| logger   | UNIX only, uses the UNIX syslog facility (/usr/bin/logger) to log information or send messages.                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |
| lp       | UNIX only, prints the notification.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |
| mail     | UNIX only, sends an email to the specified user.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |
| smtpmail | Windows only, sends an email to the specified user.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |
| nsrtrap  | Sends notifications to an SNMP management console. Use with the following options: <ul style="list-style-type: none"> <li>• -c community (if not specified, then the default public is used)</li> <li>• -f file (reads message from a file and sends as snmp trap.)</li> <li>• -i version (if not specified, then the default version is SNMPV2)</li> <li>• -s specific (default is NetWorker enterprise assignment, which is 1)</li> <li>• -t trap (default trap is #6 which is the enterprise-specific trap)</li> <li>• -u snmp uptime</li> <li>• -v verbose</li> </ul> |

Third-party programs can also be used for the action, as long as the programs support reading from standard input.

For example:

- On UNIX systems, you can use a third-party email program rather than the mail program.
- On Windows systems, you can use a third-party email program rather than the smtpmail program to send the information to other locations, such as an email address or pager system.

Only users who belong to the NetWorker server Administrators list, or a member of the Application Administrators user group, can change the Action attribute of an existing notification.

## Using nsrlpr to print notifications

NetWorker Server, on Windows systems only, looks at the printer named in each of these two sources to determine which to use to print notifications with nsrlpr:

- The Printer attribute in the Group resource. This entry is ignored if a printer is named in the Action attribute for a notification.
- The printer named in the Action attribute for a notification, or that you specified by using the -P option of the nsrlpr program.

## Designating a printer for a Notification Resource

### Procedure

1. From the **Administration** window, click **Configuration**.
2. Click **Notifications**.
3. Right-click a notification, then select **Properties**. The **Properties** dialog box appears.
4. In the **Action** attribute, type:

`nsrlpr -P printer_name`

where `printer_name` is the name of the designated printer.

If the printer name has spaces, such as eng printer one, then enclose the printer name in double quotes, as shown here:

```
nsrlpr -P "eng printer one"
```

If the printer is associated with a particular server, as is the case with Microsoft LAN Manager printers, use this syntax:

```
nsrlpr -P \\server_name\printer_name
```

where:

- `server_name` is the name of the server to which the printer is attached.
- `printer_name` is the name of the printer to use.

## Sending the bootstrap notification printout to its group's printer

To send the bootstrap notification printout to the printer defined in the Printer attribute of the Group resource:

### Procedure

1. From the **Administration** window, click **Configuration**.
2. Click **Notifications**.
3. Right-click **Bootstrap**, then select **Properties**. The **Properties** dialog box appears.
4. In the **Action** attribute, type:

```
nsrlpr -P %printer
```

## Testing the nsrlpr program

To test the nsrlpr program, type:

```
nsrlpr -P printer_name text_file
```

where:

- `printer_name` is the name of the printer to use.
- `text_file` is the name of a text file to print.

The printer name was typed incorrectly if you receive this error message:

```
Error: print server did not accept request. Job aborted.
```

Once you can print from the command prompt, enter this command to change the Action attribute to the print command:

```
nsrlpr -P printer_name
```

**NOTICE**

Print jobs sent by the NetWorker Backup and Recover Server service run in the Local System context. Under certain conditions, it may not have access to network print queues. Microsoft Knowledge Base articles 132679 and 143138 on the Microsoft web site provide more information.

## Using `smtpmail` to email notifications

Use the `smtpmail` program included with the NetWorker software on Windows systems to email an event notification to a list of specified e-mail addresses.

The `smtpmail` program requires:

- A mail server that allows SMTP relays.
- An active TCP/IP connection. This command does not have dialing capabilities.

The `smtpmail` command reads message sent from standard input.

The message is terminated in one of the following ways:

- An EOF.
- CTRL-Z on console.
- A line consisting of a single period (.)

To use the `smtpmail` program to email event notifications:

### Procedure

1. From the **Administration** window, click **Configuration**.
2. Click **Notifications**.
3. Right-click on the notification, then select **Properties**. The **Properties** dialog box appears.
4. In the **Action** attribute, type:

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

where:

- **-ssubject** — includes a standard e-mail header with the message and specifies the subject text for that header. Without this option, the `smtpmail` program assumes that the message contains a properly formatted e-mail header and nothing is added.
- **-hmailserver** — specifies the hostname of the mailserver 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.
5. Click Ok.

## Priorities

Each NetWorker event has a series of associated messages, and each message has an associated priority. The preconfigured notifications have selected priorities based on the importance of the message being sent. For example, the first time the NetWorker server sends a mount backup volume request, the priority assigned to the message is Waiting. The priority of the second request is Alert. The priority of the third request is Critical.

The following table lists the priorities upon which notifications are based.

**Table 86** Priorities

| Priority    | Description                                                                                                  |
|-------------|--------------------------------------------------------------------------------------------------------------|
| Information | Information about the current state of the server.                                                           |
| Notice      | Important information.                                                                                       |
| Warning     | A non-fatal error has occurred.                                                                              |
| Waiting     | The NetWorker server is waiting for an operator to perform a routine task, such as mounting a backup volume. |
| Alert       | A severe condition exists that requires immediate attention.                                                 |
| Critical    | The server detected an error that should be fixed.                                                           |
| Emergency   | A condition exists that may cause NetWorker to fail unless corrected immediately.                            |

**NOTICE**

Event priorities are sorted alphabetically, rather than by severity.

## Logging event notifications

NetWorker keeps two general notification log files. By default, these files are located in <NetWorker\_install\_dir>\logs:

- The messages log file (Windows only) — The data in the messages log file is generated by nsrlog, a program that is part of the NetWorker event notification mechanism. The nsrlog program is triggered by a notification, and it prints the message to the messages log file.
- The daemon.raw log file — The nsrd, nsrexd, and their subordinate processes redirect their output to the daemon.raw log file.

[Viewing log files on page 677](#) provides information about viewing log files.

To better access and use these event logs on Windows systems, an Event Logging mechanism enables applications to the application event log, and access them from any computer that has the Windows Event Viewer. The Event Viewer enables you to look selectively at the messages that interest you by filtering messages based on the categories listed in this table.

**Table 87** Event Viewer messages

| Event Viewer category | Displayed information                                                                                                                                                                                                                                                                  |
|-----------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Source                | Events from NetWorker software always designate NetWorker as the source.                                                                                                                                                                                                               |
| Category              | Mapped from NetWorker notification event type (savegroup, server, registration, and so on).                                                                                                                                                                                            |
| Severity              | Mapped from NetWorker notification priority: <ul style="list-style-type: none"> <li>• Critical and Emergency are mapped to Error.</li> <li>• Priorities between Alert and Warning are mapped to Warning.</li> <li>• Notification and Information are mapped to Information.</li> </ul> |
| Event ID              | Events from NetWorker software always designate the numeral 1 for the ID.                                                                                                                                                                                                              |

## Creating a custom notification

NetWorker also provides preconfigured notifications. [Preconfigured notifications on page 446](#) provides a complete list of preconfigured notifications.

### Procedure

1. From the **Administration** window, click **Configuration**.
2. Right-click **Notifications**, then select **New**. The **Create Notification** dialog box appears.
3. In the **Name** attribute, enter a name for the notification.
4. In the **Event** attribute, select the events to be acted on.
5. In the **Priority** attribute, select the priorities of the corresponding actions.
6. In the **Action** attribute, enter a command to execute in response to the selected events and priorities.
7. Click **Ok**.

## Editing a notification

### NOTICE

---

You cannot change the name of a notification.

---

### Procedure

1. From the **Administration** window, click **Configuration**.
2. Click **Notifications**.
3. Right-click the notification to edit, then select **Properties**. The **Properties** dialog box appears.
4. Make any required changes, then click **Ok**.

## Copying a notification

### Procedure

1. From the **Administration** window, click **Configuration**.

2. Click **Notifications**.
3. Right-click the notification to copy, then select **Copy**. The **Create Notification** dialog box appears, containing the same information as the notification that was copied, for **Name** attribute.
4. In the **Name** attribute, enter a name for the new notification.
5. Edit any other attributes as appropriate, then click **Ok**.

## Deleting a custom notification

**NOTICE**

You cannot delete any of the preconfigured notifications.

### Procedure

1. From the **Administration** window, click **Configuration**.
2. Click **Notifications**.
3. Right-click the notification to delete, then select **Delete**.
4. When prompted, click **Yes** to confirm the deletion.

## Configuring owner notifications

Owner notification is an attribute of the NetWorker client resource. Use this attribute to send an email to a user with the results of the backup of the individual client.

For Windows NetWorker servers, use the **smtpmail** program to send the owner notification email. [Using smtpmail to email notifications on page 454](#) describes how to configure the **smtpmail** program.

For UNIX NetWorker servers, use the **/usr/ucb/mail** program or a third-party mail application to send the owner notification.

### Procedure

1. From the **Administration** window, click **Configuration**.
2. Select **Clients** in the left navigation pane.
3. Right mouse click the client and select **Properties**.
4. Select **Globals (2 of 2)**.
  - For a Windows NetWorker server, use the **smtpmail** program to configure the email notification. [Using smtpmail to email notifications on page 454](#) describes how to configure **smtpmail**.
  - For a UNIX NetWorker server, use the **/usr/ucb/mail** program:

```
/usr/ucb/mail -s "subject" recipient1@mailserver  
recipient2@mailserver...
```

For example:

```
/usr/ucb/mail -s "Backup status for client xyz in group abc"  
debbie@mymailhost.com
```

5. Click **Ok**.

### Results

When the group containing the client completes, the notification is sent to the recipient email address defined in the Owner notification attribute.

For example:

```
-----Original Message-----
From: Super-User [mailto:root@NWserver.emc.com]
Sent: Thursday, March 22, 2012 12:45 PM
To: debbie@mymailhost.com
Subject: Backup status for client xyz in group abc
cdcsdunndl1c, savefs, "succeeded:full:savefs"
* cdcasdunndl1c:savefs savefs cdcasdunndl1c: succeeded.
cdcsdunndl1c, C:\cmdcons\system32, "<NULL>:full:save"
* cdcasdunndl1c:C:\cmdcons\system32 cdcasdunndl1c:C:\cmdcons\system32
aborted
* cdcasdunndl1c:C:\cmdcons\system32 Termination request was sent to
job 64006 as requested; Reason given: Aborted
```

## Reporting group status and backup job status

When you perform a backup, clone or archive activities for clients in an active group, NetWorker records the status of the group completion and job activities. There are three way to report job activities:

- In the Monitoring window for the NetWorker server in NMC. [Monitoring NetWorker server activities on page 430](#) describes how to view the backup group completion status in the Monitoring window.
- Through predefined savegroup completion notifications. [Savegroup completion and failure notifications on page 458](#) provides more information.
- By querying the job status. [Querying the job status on page 461](#) provides more information.

## Savegroup completion and failure notifications

By default, for a UNIX NetWorker server, an email of the Savegroup completion and the Savegroup failure report are sent to the root account after all client activities of a group are finished. On Windows, the Savegroup completion and Savegroup failure details are written to a savegrp.log file located in the NetWorker\_install\_dir\logs directory. [Notifications on page 445](#) describes how to customize Savegroup completion and Savegroup failure notifications.

The following sections provide more information about the Savegroup completion and Savegroup failure notifications:

- [Format of the Savegroup completion and Savegroup failure notifications on page 458](#)
- [Customizing the save sets status in the Savegroup completion and Savegroup failure notifications on page 460](#)
- [Filtering the savegroup completion report messages on page 461](#)

### Format of the Savegroup completion and Savegroup failure notifications

The Savegroup completion and Savegroup failure notifications are divided into a number of sections that describe the job activities for a savegroup.

The sections of the Savegroup completion and Savegroup failure notifications are:

- The summary line — Provides a summary of the overall status of the savegroup. The Savegroup completion and the Savegroup failure notifications provide summaries that includes the name of the savegroup, the total number of clients that are in the savegroup, the number of clients that experienced a job failure, and the status of the clone job, when automatic cloning is enabled for the group.

For example:

```
NetWorker savegroup: (alert) Default completed, Total 2 client(s),
2 Failed. 1 Succeeded(Save Set Cloning Failed). Please see group
completion details for more information.
```

The Savegroup failure notification provides an additional summary line, reporting the number of:

- Clients in the savegroup.
- Disabled clients in the savegroup.
- Clients whose hostname cannot be resolved.
- Successful and unsuccessful BMR client backups.
- Successful and unsuccessful checkpoint-enabled client backups.

For example:

```
NetWorker savegroup failure: (alert) Default Completed/Aborted,
Total 7 client(s), 1 Clients disabled, 1 Hostname(s)
Unresolved, 2 Failed, 1 Succeeded, 1 CPR Failed, 1 CPR
Succeeded, 1 BMR Failed, 1 BMR Succeeded.
```

- The summary body — Provides more detailed information about the jobs in a savegroup including:
  - The Start time of the savegroup.
  - The Restart time of the savegroup. This only appears if the savegroup was restarted.
  - The Clone start time of the savegroup. This only appears if automatic cloning is enabled for the savegroup.
  - The End time of the savegroup.
  - A list of hostnames that experienced a job failure and the type of failure.

```
hostname resolution failed for 1 client(s)
Unresolved: myfailedclient1.emc.com
Failed: myfailedclient1.emc.com, myfailedclient2.emc.com
Disabled: mydisabledclient.emc.com
Failed after CPR: mycprfailed.emc.com
BMR Failed:myfailedBMR.emc.com
Succeed with warning(s) :mywarnings.emc.com
Succeeded: mysuccess.emc.com
Start time: Thu Apr 19 16:45:55 2012
Clone Start: Thu Apr 19 16:50:55 2012
End time: Thu Apr 19 16:55:22 2012
Automatic cloning of save sets to pool Default Clone failed.
```

- The save set status section is divided into six status categories:
  - Never started save sets — Provides a summary of save sessions that were not started.
  - Unsuccessful Save Sets — Provides a summary of finished save sessions that are considered unsuccessful or incomplete. Save sets that complete with warnings are considered unsuccessful when the Success threshold attribute for the savegroup resource is set to Success. [Customizing the save sets status in the Savegroup completion and Savegroup failure notifications on page 460](#) provides detailed information about configuring the Success threshold attribute.
  - Successful Save Sets — Provides a summary of finished save sessions that are considered successful.

- Succeeded With Warnings — Provides a summary of finished save sessions that are considered successful but encountered warnings. Save sessions that finish with warnings are considered successful when the Success threshold attribute for the savegroup resource is set to Warning. [Customizing the save sets status in the Savegroup completion and Savegroup failure notifications on page 460](#) provides detailed information about configuring the Success threshold attribute.
  - Cloned Save Sets — Provides the status of the clone job. This section only appears when automatic cloning is enabled for the savegroup.
  - Succeeded In Previous Runs — Provides a summary of save sessions that succeeded in a previous backup attempt of the savegroup. This section only appears when a save group is restarted after a previous failure.
- For example:

```

--- Never Started Save Sets ---
* client1:D:\ save was never started
--- Unsuccessful Save Sets ---
* myfailed_client:index 90018:save: Cannot open a save session
with NetWorker server 'bu-t3-7.lss.emc.com': no matching
devices for save of client 'bu-t3-7.lss.emc.com'; check storage
nodes, devices or pools
* myfailed_client:index cdcstdunndll1c:index: retry #1
* myfailed2_client:bootstrap 90018:save: Cannot open a save
session with NetWorker server 'myfailed2_client': no matching
devices for save of client 'bu'; check storage nodes, devices
or pools
myfailed2_client:bootstrap: retry #1
--- Successful Save Sets ---
* mysuccesful_client:savefs savefs mysuccesful_client:
succeeded.
* mysuccesful_client C:\cmdcons           level=full,    7949 KB
00:00:05      183 files
* mysuccesful_client:C:\cmdcons completed savetime=1334782210
--- Cloned Save Sets ---
Automatic cloning of save sets to pool Default Clone failed.

```

## Customizing the save sets status in the Savegroup completion and Savegroup failure notifications

How the status of the save sessions is reported in Savegroup completion and Savegroup failure notifications is determined by the value that is defined in Success threshold for the group. Consider the following:

- The Success threshold value is defined under the Advanced tab of the Group Properties window.
- When the Success threshold is set to:
  - Warning — Any save set that completes with warnings will be reported as successful. This is the default value.
  - Success — Any save set that completes with warnings is considered to have failed and is reported as unsuccessful. Failed save sets are retried according to the value defined in the Client Retries attribute, also located under the Advanced tab of the Group Properties window.
- The Success threshold attribute also applies to the save sets displayed in the Completed successfully and Failed sections of the Group details window. [Viewing group backup details on page 434](#) provides more information about viewing group backup details.

## Filtering the savegroup completion report messages

The nsrscm\_filter command provides the ability to filter the savegroup completion messages on a UNIX or Linux NetWorker server based on a user defined filter file.

There are a number of ways to use the nsrscm\_filter command to filter savegroup completion messages in NetWorker:

- Modify the action attribute of the savegroup completion notification to direct the output to a savegrp log file. Use the nsrscm\_filter program to filter the savegrp log file.

The nsrscm\_filter program is located in the following directory by default:

- Solaris and Linux: /usr/sbin/
- HPUX: /opt/networker/bin
- AIX: /usr/bin

- Modify the action attribute of the savegroup completion notification to use the nsrscm\_filter program and generate a filtered savegrp log file.

For example:

```
name: savegroup completion report;
action: /usr/sbin/nsrscm_filter -f  /nsr/res/filter_msgs      -l 2
-D 1    -s /nsr/logs/scm/savegrp.$$      -o /nsr/logs/scm/
scmfilter.$$ ;
event: Savegroup;
priority: alert, notice;
```

where filter\_msgs is the user defined filter file. A template filter file filter\_msgs.templ is provided in the same location as the nsrscm\_filter program.

[Editing a notification on page 456](#) describes how to modify preconfigured notifications.

- Modify the action attribute of the savegroup completion notification to call a script that runs the nsrscm\_filter command and sends the filtered output in an email. A template script file, scm-notification.sh is provided in the same location as the nsrscm\_filter program.

The *EMC NetWorker 8.0 Command Reference Guide* and the UNIX man pages provide nsrscm\_filter usage information.

## Querying the job status

When a backup, clone or archive job is run within an active savegroup, job information is stored in savegrp log files and the jobs database (jobsdb) on the NetWorker server host.

Before you query job status, review this information:

- NetWorker logs details of the corresponding savegroup's child jobs into text files located in:  
NetWorker\_install\_dir\nsr\logs\sg\savegroup\_name\Job\_ID  
where Job\_ID is the file whose name corresponds to a savegroup child job ID.

### Note

In NetWorker 7.6.x, Savegroup log by job id was a configurable option and not enabled by default. In NetWorker 8.0 and higher, **Savegroup log by job id** is the default behaviour and is not configurable.

- The job files are purged based on value of the Jobsdb retention in hours attribute in the properties of the NetWorker server resource. Prior to NetWorker 8.0, the job files were overwritten each time the group started.
- Each jobs file contains the output that the job returns to stderr or stdout.
- The jobsdb stores the savegroup completion information. Prior to NetWorker 8.0 NetWorker stored the Savegroup completion information in the Completion attribute of the Group resource in the resource database of the NetWorker server.

The NetWorker software provides two command line programs to query job information.

- [Using jobquery on page 462](#)describes the jobquery program that is used to locate and retrieve information about all jobs including the child jobs of a savegroup.
- [Using nsrsgrpcomp on page 463](#) describes how to use the nsrsgrpcomp program to query savegroup specific information from the job database. Use this program to retrieve completion information that was stored in the resource database in previous versions of NetWorker.

The man pages or the *EMC NetWorker Command Reference Guide* provides more information on the `jobquery` and `nsrsgrpcomp` commands.

## Using jobquery

The jobquery program provides an CLI similar to the nsradmin program. The jobquery program contacts the nsrjobd process to query job information stored in the jobsdb. A query is defined by an attribute list that is made up of one or more attribute names with or without values.

In the query, the attribute name (for example, 'type') is preceded by a '.', and optionally followed by a ':' and a comma-separated list of values (for example, "host: mars";"job state: STARTED, ACTIVE, SESSION ACTIVE"). When a query consists of more than one attribute names, attributes are separated by a ';'. When an attribute name is specified without values, any resource descriptor that contains this attribute is a match. If an attribute name is followed by one or more values, a resource whose value list matches at least one of the values for the specified attribute satisfies the criteria.

To launch the jobquery interface, type the following command:

```
jobquery -s NetWorker_server
```

If the `-s NetWorker_server` option is not used, jobquery attempts to connect to nsrjobd process on the local host. If the nsrjobd process is not running on the specified server or the local host, an error is returned.

The `jobquery -s <server>` command connects to the specified NetWorker server and returns jobquery prompt. The data in the job database is queried with the following commands:

- `types` — a command that lists all job types currently known by nsrjobd that does not take any argument (for example, `types` will return a list indicating Known types: save job, savegroup job, and so on).
- `. —` a command that sets the query criteria and is followed by one or more attribute names, or lists current query criteria when not followed by any attribute. Query criteria may contain several attributes, including job type, host, and job state, with each attribute separated by a semi-colon and each value separated by a comma, as in the following example:

```
jobquery> . type: savegroup job; host: mars; job state: ACTIVE, COMPLETED
```

The above example would return information on all savegroup jobs from the machine mars that are either in progress or in completed state.

- show — restricts the list of attributes returned for each resource descriptor that matches the query. For the above example, specifying the following:

```
show name; job id; completion status; completion severity
```

will return the names, job ids, completion status and completion severity for all matched completed and active savegroups.

- print — executes the query and displays the results. If show list is in effect, each resource descriptor in the result list is restricted to desired attributes.
- all — returns all resource descriptors in the jobs database. If show list is in effect, result is restricted to desired attributes.
- help — displays help text.
- quit — exits jobquery.

Running `jobquery -s NetWorker_server -i input_file` reads input from the file for non-interactive usage. The man pages or the *EMC NetWorker Command Reference Guide* provides detailed information about the jobquery program.

## Using nsrsgrpcomp

Similar to the jobquery program, the nsrsgrpcomp program queries information stored in the jobsdb. The nsrsgrpcomp program differs from the jobquery program because it also queries savegrp log files and is limited to savegrp job information only.

Use the nsrsgrpcomp program to:

- Provide savegroup completion output.
- Retrieve all job details for a group including save set status.
- Retrieve all job details for a client in a group.
- Retrieve all savegroup job details in the jobs database.

Example: View the completion report

To generate the completion report that was previously stored in the completion attribute for a savegroup in the resource database of the NetWorker server, type:

```
# nsrsgrpcomp -b -1 group_name
```

where `-b -1` is optional and used to override the default 2kb limit for job output.

Example: Summary of last savegroup backup

To generate a summary of the savegroup jobs for the last run of a savegroup run, type:

```
# nsrsgrpcomp -H group_name
```

For example, to generate a summary report of the last run of the Default savegroup:

```
nsrsgrpcomp -H Default
bu-t3-7.lss.emc.com, bootstrap, "failed:full:bootstrap"
cdcsdunndl1c, savefs, "succeeded:full:savefs"
cdcsdunndl1c, C:\cmdcons\system32, "succeeded:incr:save"
cdcsdunndl1c, index, "failed:full:index"
```

Example: Query the savegroup status

To query the jobs database for a status of a previous run of a savegroup:

1. Use `nsrsgrpcomp -L` to report a summary of all jobs stored in the jobs database.

2. For example:

```
nsrsgrpcomp -L Default
name, start time, job id, previous job id, completion status
Default, Tue Apr 17 10:40:04 2012(1334673604), 160023, 0, failed
Default, Tue Apr 17 14:15:46 2012(1334686546), 160033, 0, failed
```

3. Use **nsrsgrpcomp** with the **-t** option and the **start time** value associated with the savegroup.

```
nsrsgrpcomp -b -1 -t "Tue Apr 17 10:40:04 2012" Default
bu-t3-7.lss.emc.com, bootstrap, "failed:full:bootstrap"
* bu-t3-7.lss.emc.com:bootstrap Failed with error(s)
* bu-t3-7.lss.emc.com:bootstrap 90018:save: Cannot open a save
session with NetWorker server 'bu-t3-7.lss.emc.com': no matching
devices for save of client `bu-t3-7.lss.emc.com'; check storage
nodes, devices or pools
cdcsdunndl1c, savefs, "succeeded:full:savefs"
* cdcsdunndl1c:savefs savefs cdcsdunndl1c: succeeded.
cdcsdunndl1c, C:\cmdcons\system32, "succeeded:incr:save"
* cdcsdunndl1c:C:\cmdcons\system32 cdcsdunndl1c: C:\cmdcons
\system32 level=incr, 0 KB 00:00:03 0 files
* cdcsdunndl1c:C:\cmdcons\system32 completed savetime=1334587461
cdcsdunndl1c, index, "failed:full:index"
* cdcsdunndl1c:index Failed with error(s)
* cdcsdunndl1c:index 90018:save: Cannot open a save session with
NetWorker server 'bu-t3-7.lss.emc.com': no matching devices for
save of client `bu-t3-7.lss.emc.com'; check storage nodes, devices
or pools
```

The man pages or the *EMC NetWorker Command Reference Guide* provides detailed information about the nsrsgrpcomp program.

## Reporting recover job status

When you perform a recover by using the NMC Recovery Wizard, NetWorker records the status of the recover operation and job activities. There are two ways to report job activities:

- In the Recover window for the NetWorker server in NMC. [Monitoring NetWorker server activities on page 430](#) describes how to view the Recover status in the Recover window.
- By querying the job status by using nsrrecomp command on the NetWorker server. [Using nsrrecomp on page 464](#) provides more information.

## Using nsrrecomp

Use the nsrreccomp program to query the jobsdb for information about recover jobs and to create a recover completion report. The name given to the recover job is the name of the saved recover configuration. The nsrreccomp program differs from the jobquery program because it also queries recover log files and is limited to recover job information only.

**Example: Summary report of recover jobs**

To generate a summary report of each recover job in the jobsdb, type:

```
nsrreccomp -L
```

**Example: Recovery job completion report**

To generate a completion report for recover job, type:

```
nsrreccomp -b -1 recover_job_name
```

where -b -1 is optional and used to override the default 2kb limit for job output.

Example: Summary report of the last recovery job

To generate a summary of last recovery job for a recover resource, type:

```
nsrreccomp -H group_name
```

The man pages or the *EMC NetWorker Command Reference Guide* provides detailed information about the nsrsreccomp program.



# CHAPTER 17

## NMC Server Management

This chapter contains the following topics:

- [NMC server authentication](#)..... 468
- [Moving the NMC server](#)..... 468
- [Setting system options to improve NMC server performance](#)..... 470
- [Setting environment variables](#)..... 473
- [Using the NMC Configuration Wizard](#)..... 474
- [NetWorker NMC server maintenance tasks](#)..... 474
- [Displaying international fonts in non-US locale environments](#)..... 477
- [NetWorker License Manager](#)..... 477

## NMC server authentication

When you use a web browser on a host (NMC client) to connect to the NMC server, the http daemon on the NMC server downloads the Java client to the NMC client. You do not require a secure http (https) connection because only the Java client transfers information and performs authentication between the NMC server and NMC client. The NMC server uses SSL to encrypt the username and password that you specify in the login window. The first time that you connect to the NMC server the NMC Configuration Wizard prompts you to specify a password for the administrator user. On subsequent log in attempts, the NMC server authenticates the credentials by using Native NMC-based user authentication. NMC supports the use of an external authentication authority, for example, Lightweight Directory Access Protocol over SSL (LDAPS), or a Microsoft Active Directory server (AD).

The *EMC NetWorker Security Configuration Guide* describes how to perform the following tasks:

- Managing native NMC-based authentication, including how to reset the administrator password
- Configuring NMC to use an external authentication authority
- Configuring user authorization to the NMC and NetWorker servers

## Moving the NMC server

You can move a NMC server from one host to another only if both hosts use the same operating system.

### Procedure

1. Backup the existing NMC database with the `savepsm` command at level **Full**.  
[Performing a manual backup of the Console database on page 105](#) provides more details.
2. Setup the new host with the same operating system as the host that runs the current software and connects to the network.
3. On the new host, install the NetWorker Client software and the NMC server software.

#### NOTICE

If you use a License Manager server, then install and configure the License Manager software first. If you use the License Manager software and the License Manager server moves to a new host, then specify the new License Manager hostname in the Console window.

4. On the NetWorker server, setup the new target host as a client resource. [Creating a backup Client resource on page 65](#) describes how to create a Client resource.
5. Edit the Client resource of the source NMC server and add the appropriate users to the **Remote Access** attribute on the **Globals (2 of 2)** tab.
6. Stop the NMC server service on the source NMC server.
7. Stop the NMC server service on the target NMC server.
8. Ensure you stop the GST service on the original backup host or on the host used for the directed recover. Use the appropriate command or tools for the operating system to ensure the GST service is not running.

9. For UNIX systems, update the library path environment variable with the NMC server library path.

- On AIX, update the LIBPATH variable with `NMC_install_dir/sybasa/lib64` where `NMC_install_dir` is `/opt/LGTONMC` by default.
- On Linux and Solaris, update the `LD_LIBRARY_PATH` variable with `NMC_install_dir/sybasa/lib` where `NMC_install_dir` is `/opt/LGTONMC` by default.

**NOTICE**

If you did not install the NMC server software in the default location, then add `/NMC_install_dir/bin` to the library path environment variable.

10. On the NetWorker server, you must have:

- Client resources for the original backup host and the directed recover host.
- The root or administrator account of the directed recover host listed in the **Remote Access** field of the client resource for the original backup host.

11. Run the `recoverpsm` command on the recovery host:

```
recoverpsm [-f] [-d recover_directory] -s NetWorker_server -c
original_NMC_server -S gst_on_original_console_server -0
```

For example,

- To recover the NMC server database and `gstdb.conf` credential file to the original backup location on the directed recover host, type this command:

```
recoverpsm -f -c original_NMC_server_hostname
```

- To recover the NMC server database and `gstdb.conf` credential file, to a directory on the directed recover host that differs from the original backup location type this command:

```
recoverpsm -c original_NMC_server_hostname -f -d recover_
directory
```

The following table provides a description of `recoverpsm` options. The *EMC NetWorker Command Reference Guide* or the UNIX man pages provide a complete description of the `recoverpsm` command line options.

**Table 88** The `recoverpsm` options

| Option                            | Meaning                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |
|-----------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <code>-f</code>                   | Instructs the software to overwrite existing NMC database files.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |
| <code>-d recover_directory</code> | Specifies the destination directory for the recovered NMC database and if you did not specify the <code>-O</code> option, the destination directory of the <code>gst_db.conf</code> configuration file. Include a full path for the directory. The recover process does not support partial paths. When the <code>recover_directory</code> is not the same as the console database directory, copy the database file and the <code>gst_db.conf</code> file, to the directory where the console database resides after the recovery operation completes. |

**Table 88** The recoverpsm options (continued)

| Option                                   | Meaning                                                                                                                                                                                                                                                                                              |
|------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <code>-S gst_on_source_NMC_server</code> | Specifies the existing NMC database on the source NMC server. You must prepend <code>gst_on_</code> to the short name of the source NMC server.                                                                                                                                                      |
| <code>-O</code>                          | Do not recover the database credential file, <code>gstd_db.conf</code> . Use this option to preserve preexisting database login credentials on recovery server. Use the recover program or the NetWorker User program to recover the <code>gstd_db.conf</code> configuration file to a new location. |
| <code>-s NetWorker_server</code>         | Specifies the name of the NetWorker server where the NMC database backup resides.                                                                                                                                                                                                                    |
| <code>-c source_NMC_server</code>        | Specifies the short name of the source NMC server, where the existing NMC database resides.                                                                                                                                                                                                          |

- 12.If you use LDAP authentication, then recover the LDAP configuration authority files. Use the `recover` command, the NetWorker User program or the NMC Recovery Wizard to recover all the files in the `console_install_dir/cst` directory. Recover these files to the `console_install_dir/cst` directory on the target NMC server.
- 13.Start the NMC server program on the target NMC server.
- 14.If you use the License Manager and the License Manager host has changed, obtain a Host Transfer Affidavit from EMC Licensing. Use the host ID of the License Manager host for the new authorization codes. If the License Manager host has not changed, then new authorization codes are unnecessary.

## Setting system options to improve NMC server performance

The NMC server includes several options that enable users to fine-tune the performance of the NMC server.

To set system options, log in to the NMC server as a Console administrator.

### Procedure

1. From the **Console** window, click **Setup**.
2. From the **Setup** menu, select **System Options**.
3. Set a value, or enable or disable the appropriate system option. The following table provides a description of the available system options.

#### NOTICE

Do not adjust these system options without careful consideration. A mistake in setting system options can seriously degrade performance.

**Table 89** NMC server system options

| System option | Description                                  |
|---------------|----------------------------------------------|
| Log-on banner | Default Value: Warning: Authorized user only |

**Table 89** NMC server system options (continued)

| System option                                       | Description                                                                                                                                                                                                                                                                                                                                                                                               |
|-----------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|                                                     | Defines the log-on banner displayed in the NMC server login window.                                                                                                                                                                                                                                                                                                                                       |
| Debug level                                         | <p>Default value: 0<br/>Range: 1-20</p> <p>Defines the level of debug information to log in the gstd.raw file. Increase this value to troubleshoot only.</p>                                                                                                                                                                                                                                              |
| Polling interval for events and reporting (seconds) | <p>Default value: 20<br/>Range: 0-20</p> <p>Defines how frequently the NMC server contacts the managed NetWorker servers for event and report updates.</p>                                                                                                                                                                                                                                                |
| Polling interval for NetWorker activities (seconds) | <p>Default value: 10<br/>Range: 0-20</p> <p>Defines the frequency in which the NMC server contacts the managed NetWorker servers for activity updates.</p>                                                                                                                                                                                                                                                |
| Polling thread factor                               | <p>Default value: 5<br/>Range: 0-20</p> <p>Defines how many server threads to create when polling the NetWorker server for NetWorker activities, events, and reporting. The higher the number the higher the number of threads created. It is not a one-to-one relationship.</p>                                                                                                                          |
| Polling interval for NetWorker libraries (hours)    | <p>Default value: 12<br/>Range: 0-20</p> <p>Defines how frequently the Console GUI polls the Libraries defined for a NetWorker server to gather information. This information appears in Libraries task of the main Console GUI window.</p>                                                                                                                                                               |
| Maximum number of log messages                      | <p>Default value: 32<br/>Range: 32-512</p> <p>Defines the number of log messages that display in the Console Log window.</p>                                                                                                                                                                                                                                                                              |
| NetWorker user auditing                             | <p>Default value: disabled</p> <p>When enabled, the NMC server collects auditing information. For example, NetWorker server configuration changes performed from the Console GUI. The NMC server database stores the auditing information. To view audit information browse to Reports &gt; Users &gt; User Audit Report.</p> <p>When disabled, the NMC server does not collect auditing information.</p> |
| User authentication for NetWorker                   | <p>Default value: enabled</p> <p>Defines how the Console user accesses a managed NetWorker server.</p>                                                                                                                                                                                                                                                                                                    |

**Table 89** NMC server system options (continued)

| System option                                 | Description                                                                                                                                                                                                                                                                                                                                                                                                                                              |
|-----------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|                                               | <ul style="list-style-type: none"> <li>When enabled, the Console username determines the Console user access. <a href="#">Individual User Authentication on page 472</a> provides detailed information.</li> <li>When disabled, the user id of the gstd process owner determines the Console user access.</li> </ul>                                                                                                                                     |
| RPC ping via UDP when connecting to NetWorker | <p>Default value: enabled<br/>Before the NMC server connects to a managed NetWorker server, the NMC server confirms that the NetWorker server daemons are running.</p> <ul style="list-style-type: none"> <li>When enabled, the NMC server uses the UDP protocol to confirm that the NetWorker server is up and running.</li> <li>When disabled, the NMC server uses the TCP protocol to confirm that the NetWorker server is up and running.</li> </ul> |

- Click OK.

## Individual User Authentication

Console security administrators restrict or grant Console user access to NetWorker servers based on the Console username when you enable the User Authentication for NetWorker system option, after a subsequent restart of the NMC server service. The NMC server software enables this system option by default.

Requests to NetWorker servers through the Administration window always come from the NMC server, regardless of any system option settings.

When you enable the User Authentication for NetWorker system option:

- Access requests to a NetWorker server appear to be coming from users on the NMC server, rather than from the gstd process owner on the NMC server.
- A NetWorker server allows requests only from users who belong to the Administrators list of the NetWorker server. You must include the username of the Console daemon process owner in the NetWorker Administrators list on NetWorker servers to which Console users have access. The *EMC NetWorker Installation Guide* describes how to add the Console daemon process owner to the NetWorker Administrators list by using the nsraddadmin command.

**NOTICE**

You must specify the username of the root or system user on the NMC server, regardless of whether you use individual user authentication.

## Impact on network connections

When you enable individual user authentication, the NMC server software might require more network connections. Additional network connections might firewall port requirements. The *EMC NetWorker Security Configuration Guide* provides information about firewalls.

When you set the User Authentication for NetWorker system option, the NMC server software creates a separate network connection the NMC server to a NetWorker server for each Console user that has an Administration window open to that server.

When you do not set the user authentication for NetWorker system option, there is only one network connection from the NMC server to the managed NetWorker server.

## Setting environment variables

The following table describes the NMC server environment variables available in this NetWorker release. The environment variable values are incorporated only when the NMC server checks for environment variables at start, similar to how the nsrd daemon handles its corresponding variables.

To set environment variables in the gst file, use a Bourne shell script on UNIX systems.

**Table 90** Console environment variables

| Environment variable | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             |
|----------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| GST_DEBUG            | Range: 1–20 Default: 0<br>Use this environment variable to troubleshoot the product when the Console GUI is not accessible. This environment variable: <ul style="list-style-type: none"> <li>Defines the level of debug information written to the gstd.raw log file.</li> <li>Overrides the Debug Level attribute defined in System Options. Setting the value higher increases:</li> <li>The number of operation and status messages that the NMC server records.</li> <li>The size of the gstd.raw file.</li> </ul> |
| GST_RESET_PW         | Resets the default administrator password for native NMC authentication. <a href="#">Moving the NMC server on page 468</a> provides detailed information.                                                                                                                                                                                                                                                                                                                                                               |
| GST_RESET_DBPWD      | Changes the database connection credentials. <a href="#">Changing database connection credentials on page 475</a> provides detailed information.                                                                                                                                                                                                                                                                                                                                                                        |

## Setting environment variables on UNIX

Perform the following steps from a system prompt on the NMC server.

### Procedure

- Change the file permissions. By default, the gst file is a read-only file. The file location varies depending on the operating system:
  - Solaris and Linux: /etc/init.d/gst
  - AIX: /etc/rc.gst
- Open the file in a text editor and add these lines to the beginning of the file:

```
variable_name=variable_value
export variable_name
```

where:

- variable\_name* is the name of the environment variable.

- *variable\_value* is the value to assign to the environment variable.
3. Save the changes.
  4. Stop and restart the NMC server (gstd) program. [Table 9 on page 54](#) provides detailed instructions.
- 

**Note**

The preceding example is for the Bourne shell. For other shells, refer to the shell-specific documentation or man pages that describe how to set an environment variable.

---

## Setting environment variables on Windows systems

Use the Control Panel System applet on the NMC server to set environment variables.

**Procedure**

1. Browse to **Control Panel** -> **System and Security** -> **System** -> **Advanced System Settings**.
2. In the **General** tab click **Environment Variables...**
3. Click the **New** button.
4. Specify the name and value of the environment variable. Refer to [Table 90 on page 473](#) for a list of GST environment variables.
5. Stop and start the NetWorker Remote Exec and EMC gstd services in order for the environment variables to take effect.

## Using the NMC Configuration Wizard

You can use the NMC Configuration wizard to set the Administrator password, specify which NetWorker server will back up the Console database, and add NetWorker servers to the Enterprise.

Connect to the NMC server as Console Application and perform the following steps.

**Procedure**

1. From the **Console** window, click **Setup**.
2. From the **Setup** menu, select **Configuration Wizard**.

## NetWorker NMC server maintenance tasks

This section provides detailed information about maintenance tasks associated with the NMC server.

### Changing the service port used by the NetWorker Console database

By default, the NetWorker Console database uses port 2638 for TCP/IP communications. Other applications may also use this port or, as is the default installation of case with EMC AlphaStor or EMC DPA. Each application may have its own instance of the iAnywhere database installed. Having the NMC server installed on a host with one of these applications, creates a conflict.

To resolve this problem, change the service port as follows:

### Procedure

1. Stop the GST Service. [Stop and start the NMC server on page 54](#) describes how to stop the GST service.
2. Stop the service of any other products that use the iAnywhere database.
3. Ensure that `dbsrv12` processes are not running.
4. From a terminal or command prompt window, use the appropriate command, for example. `setenv` for `csh` and `export` for `sh`, to update the library path environment variable with the following location:
  - Solaris: `/opt/LGTONMC/bin:/opt/LGTONMC/sybasa/lib`
  - Linux/AIX: `/opt/lgtonmc/bin:/opt/lgtonmc/sybasa/lib`
  - Microsoft Windows (assumes default installation location):  
`C:\Program Files\EMC NetWorker\Management\GST\sybase\bin`  
 The environment variable to set varies by operating system, for example:
    - *Solaris/Linux: LD\_LIBRARY\_PATH*
    - *AIX: LIBPATH*
5. Edit the `gstd.conf` file to add or change the following line:  
`db_svc_port=port_number`  
 For example:  
`db_svc_port=2639`  
 The following locations contain the `gstd.conf`:
  - Solaris: `/opt/LGTONMC/etc`
  - Linux and AIX: `/opt/lgtonmc/etc`
  - Microsoft Windows: `C:\Program Files\EMC NetWorker\Management\GST\etc`
6. Run the `gstconfig` command to update the port value in the NetWorker NMC server configuration file. The following locations contain the `gstconfig` command:
  - Solaris: `/opt/LGTONMC/bin`
  - Linux/AIX: `/opt/lgtonmc/bin`
  - Windows: `C:\Program Files\EMC NetWorker\Management\GST\bin`
7. Close the terminal or command prompt window.
8. Start the EMC GST Service. [Stop and start the NMC server on page 54](#) describes how to start the GST service.

## Changing database connection credentials

When the NMC server starts for the first time, it automatically generates the login credentials used to log into the NetWorker Console database. The NMC server stores this information internally and the user does not need to know the required credentials. However, it may be necessary to force the NMC server to change the database connection credentials.

### Procedure

1. Stop the GST Service. [Stop and start the NMC server on page 54](#) describes how to stop the GST service.

2. Set the environment variable *GST\_RESET\_DBPWD* to any value.

For Windows system, set this value as a System Variable, then reboot the system after you set the variable.

3. Restart the GST Service. [Stop and start the NMC server on page 54](#) describes how to start the GST service.
4. Delete the *GST\_RESET\_DBPWD* environment variable. On Windows system, reboot the machine after you delete the variable.

## Updating the NMC server IP address/hostname

If you modify the IP address or hostname of the NMC server or if you add or remove protocols such as IPv6, you must update the NMC server configuration.

Perform the following steps with the root account on UNIX hosts or the administrator account on Windows hosts.

### Procedure

1. Stop the GST Service. [Stop and start the NMC server on page 54](#) describes how to stop the GST service.
2. Browse to the NetWorker bin directory then run the platform-specific commands:
  - On Windows, run `gstconfig` in the `NMC_install_dir\GST\bin` directory.
  - On Solaris, as root:
    - a. Define and export the *LD\_LIBRARY\_PATH* variable:

```
LD_LIBRARY_PATH=/opt/LGTONMC/bin:/opt/LGTONMC/sybasa/lib
export LD_LIBRARY_PATH
```

- b. Update the GST configuration:

```
./gstconfig
```

- On Linux, as root:
  - a. Define and export the *LD\_LIBRARY\_PATH* variable

```
LD_LIBRARY_PATH=/opt/lgtonmc/bin:/opt/lgtonmc/sybasa/lib
export LD_LIBRARY_PATH
```

- b. Update the GST configuration:

```
./gstconfig
```

- On AIX:
  - a. Define and export the *LIB\_PATH* variable:
 

```
LIBPATH=/opt/lgtonmc/bin:/opt/lgtonmc/sybasa/lib
export LIBPATH
```

- b. Update the GST configuration:

```
./gstconfig
```

3. Restart the EMC GST daemon. [Stop and start the NMC server on page 54](#) describes how to start the GST service.
4. For NMC server hostname changes only, delete the client resource that you created to perform NMC server database backups, then create a new client. [Scheduling backups for the Console server database on page 104](#) describes how to create and configure a client for console database backups.

## Displaying international fonts in non-US locale environments

To use or view data from a localized NetWorker server, ensure that the appropriate font is available to the NMC server.

The *EMC NetWorker Installation Guide* describes how to display international fonts on a NMC server that operates in English mode.

## NetWorker License Manager

The NetWorker License Manager (LLM) software provides centralized license management, which enables you to maintain all licenses in the enterpriseNetWorker from a single host.

With the NetWorker License Manager, you can move NetWorker software from one host to another, or change the IP address on an existing NetWorker server without having to reauthorize the software. You can install the NetWorker License Manager program as an option during the NetWorker software installation.

The latest *EMC NetWorker License Manager Installation and Administration Guide* provides more information on how to install and use the NetWorker License Manager.

### Entering an enabler code

#### Procedure

1. From the **Console** window, click **Setup**.
2. Right-click **Licensing**, then select **New**. The **Create** dialog box appears.
3. In the **Enabler Code** attribute, type the enabler code and leave the other attributes blank.
4. Click **OK**.

### Deleting an enabler code

#### Procedure

1. From the **Console** window, click **Setup** and then click **Licensing**.
2. Right-click the license to delete, then select **Delete**.
3. Click **Yes** to confirm the deletion.

### Entering an authorization code

#### Procedure

1. Log in as a Console Application Administrator.
2. From the **Console** window, click **Setup** and then click **Licensing**.
3. Right-click the license to be authorized, then select **Properties**. The **Properties** dialog box appears.
4. In the **Auth Code** attribute, enter the authorization code for the product (the authorization code assigned to the specified permanent enabler or update enabler code).
5. Click **OK**. The license is now permanently enabled.

## Changing the License Manager server

You can change the License Manager server that manages NetWorker Console licenses at any time.

### Procedure

1. Log in as a Console Application Administrator.
2. From the **Console** window, click **Setup**.
3. Right-click **Licensing**, then select **Change LLM Server**. The **Change LLM Server** dialog box appears.
4. In the **LLM Server** attribute, type the hostname of the appropriate server and click **OK**.

# CHAPTER 18

## NetWorker Server Management

This chapter contains the following topics:

|                                                                                      |     |
|--------------------------------------------------------------------------------------|-----|
| • <a href="#">Enterprise</a> .....                                                   | 480 |
| • <a href="#">Hostname changes</a> .....                                             | 487 |
| • <a href="#">Report home</a> .....                                                  | 488 |
| • <a href="#">Parallelism and multiplexing</a> .....                                 | 490 |
| • <a href="#">Managing server access</a> .....                                       | 494 |
| • <a href="#">Working with the Multi-Tenancy Facility</a> .....                      | 494 |
| • <a href="#">Resource databases</a> .....                                           | 509 |
| • <a href="#">Indexes</a> .....                                                      | 510 |
| • <a href="#">Managing Client Push</a> .....                                         | 519 |
| • <a href="#">Monitoring changes to the NetWorker and NMC Server resources</a> ..... | 523 |
| • <a href="#">Log file size management</a> .....                                     | 523 |
| • <a href="#">Internationalization</a> .....                                         | 523 |
| • <a href="#">Server communication issues within Microsoft Windows</a> .....         | 525 |

# Enterprise

The Enterprise is a visual representation of the NetWorker Console control zone. You can monitor various servers in the enterprise such as NetWorker, Data Domain, and Avamar servers for events. You can also generate various reports on events, backups, and user activity.

## Enterprise components

The Enterprise includes these components:

- **Hosts**  
A host, also known as a managed node, is the NetWorker, Data Domain, or Avamar server being monitored. A host terminates a branch in the Enterprise.
- **Folders**  
The purpose of folders is to enable the Enterprise to contain multiple levels. Each folder can contain more folders, more hosts, or more of both.

## Organizing NetWorker servers

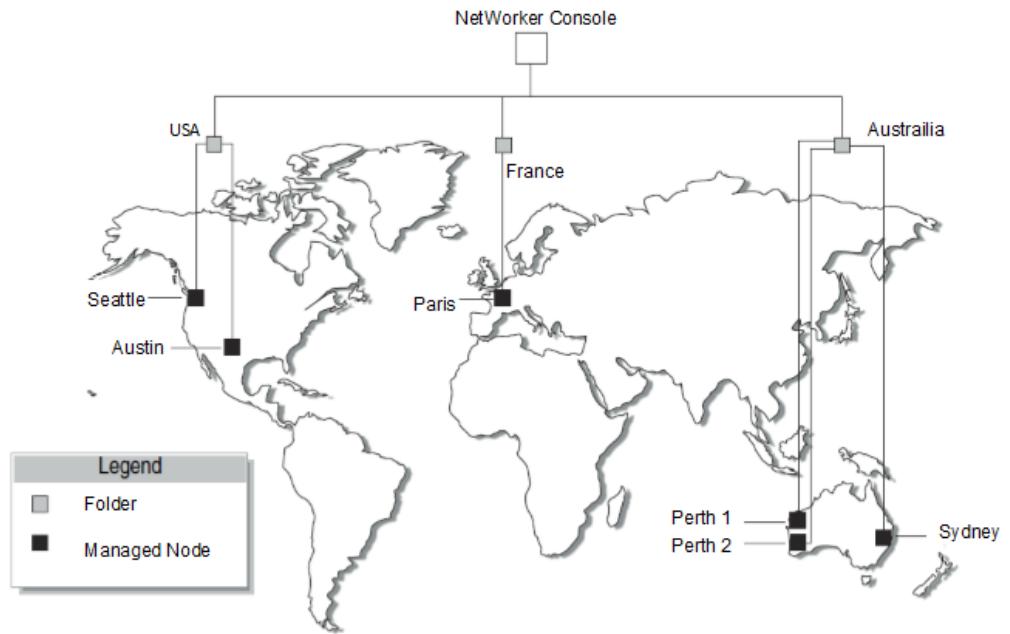
Use the Enterprise to organize the NetWorker servers by some logical or functional criteria. Examples of organizational criteria include:

- By geography. For example, you can put all of the hosts from the same city or country in the same folder.
- By function. For example, you can have the servers that back up web servers in one folder, and the servers that back up mail servers in another folder.
- By administrative divisions within the Enterprise. For example, you can use separate folders for servers that back up Marketing, Sales, or Engineering hosts.

You can create and maintain multiple folders to organize multiple copies of a host in the Enterprise. When you create each folder based on different organizational criteria, you can view the organization in different, yet parallel and complementary ways.

Example: An enterprise arranged by geographic location

This figure provides an example of an Enterprise arranged by geographic location. There are three folders, one for each country that manages NetWorker servers: USA, France, and Australia. Each folder contains a number of hosts that correspond to the location of the NetWorker servers. The Australia folder, for instance, contains three host computers labeled perth1, perth2, and sydney.

**Figure 33** NetWorker servers worldwide

## Viewing the enterprise

In the Console window, you can view the organization of the NetWorker servers in much the same way as you use a file manager program to view the contents of a file system.

### Procedure

- From the **Console** window, click **Enterprise**.
  - The left pane displays folders and hosts in a tree-like arrangement to illustrate the organization of the NetWorker servers.
  - The right pane displays the contents of the selected folder or host.
- Select a view option as described in the following table.

**Table 91** Viewing the enterprise

| To:                                                         | Perform the following action: |
|-------------------------------------------------------------|-------------------------------|
| Show or hide contents of the Enterprise.                    | Click <b>Enterprise</b> .     |
| Show or hide contents of a folder.                          | Click the folder.             |
| Show the managed applications installed on a host computer. | Click the host.               |

## Managing various servers in the enterprise

NetWorker Console enables centralized management of NetWorker, Data Domain, and Avamar servers within the Enterprise. You can use the Console window to add, delete, move, and copy servers. When you use the NetWorker software to manage a large number of NetWorker servers, you can use a single command from a command prompt to efficiently add or delete multiple hosts. [Adding or deleting multiple servers by using a hostname file on page 485](#) provides further information.

The server management activities include, but are not limited to, operations related to devices and libraries, and events that require user intervention.

## Adding a managed host

The Console window can display server events and to generate server activity-reports.

**NOTICE**

When you configure a Data Domain device with the New Device Wizard, the wizard adds Data Domain servers as a managed hosts. The *EMC NetWorker Data Domain Devices Integration Guide* provides more information about Data Domain as a managed host.

### Procedure

1. From the **Console** window, click **Enterprise**.
2. In the left pane, right-click **Enterprise**, then select **New > Host**. The **Add New Host** wizard appears.
3. Enter a hostname, IP address, DNS name, or WINS name in the **Host Name** attribute, then click **Next**.

**NOTICE**

Hostnames and aliases cannot exceed 80 characters.

4. Select the server type and click **Next**.
5. Follow the instructions for configuring selected host type, then click **Finish**.

**Note**

You can also use the **Console Configuration Wizard** to add a host.

## Deleting a host

You can delete a single host or multiple hosts within a folder.

### Procedure

1. From the **Console** window, click **Enterprise**.
2. Right-click the host to delete, then select **Delete**. The **Deleting Host** dialog box appears.
  - To delete multiple hosts, select multiple hosts in the details pane and select **Delete**.
  - If additional copies of the host exist in the Enterprise, use the **Delete all existing copies of the host** option to delete all instances of that same host in a single operation.
3. Click **Yes** to confirm deletion of the host.

## Copying a host

You can create multiple copies of a host for a single NetWorker or Avamar server. For example, you can create one copy of a host in the logical position of the host in the Enterprise, while another copy of the host is in a Hosts-to-Watch folder where you can easily monitor it. In this configuration, you can check the server without navigating through the Enterprise.

### Procedure

1. From the **Console** window, click **Enterprise**.
2. Right-click the host to copy, then select **Copy**.
3. Right-click a new location, then select **Paste**.

**NOTICE**

You can also use the drag-and-drop feature while holding down the Ctrl key to copy hosts.

---

## Moving a host

To move a host from one location to another in an Enterprise, perform the following steps.

### Procedure

1. From the **Console** window, click **Enterprise**.
2. Right-click the host to move, then select **Move**.
3. Right-click a new location, then select **Paste**.

**NOTICE**

You can also use the drag-and-drop feature while holding down the Ctrl key to move hosts.

---

## Managing folders in the enterprise

The NetWorker software allows you to manage folders within the Enterprise. This means that you can add, rename, delete, and move folders as needed.

You can add new folders directly beneath the Enterprise node or beneath other folders.

### Adding a folder

#### Procedure

1. From the **Console** window, click **Enterprise**.
2. Right-click the location within the Enterprise where you want the new folder to appear, then select **New > Folder**.  
A new folder appears in the Enterprise with the default name Untitled1.
3. Highlight the default name and type a new name to replace it. The name must meet these criteria:
  - Include at least one, but no more than 80 characters.
  - Exclude forward slashes (/).
4. Press **Enter**.

### Deleting a folder

#### Procedure

1. From the **Console** window, click **Enterprise**.
2. Right-click the folder to delete, then select **Delete**.
  - If hosts exist in the folder, a dialog box prompts you to confirm the deletion of each host. Select **Yes** to continue with the operation, or **No** to cancel it.

- If hosts do not exist in the folder, the NMC server deletes the folder.
- If the folder contains any unique hosts (meaning hosts that do not have copies anywhere else in the Enterprise), an additional dialog box appears to confirm deletion of the unique host.
 

A separate dialog box with four options appears for each unique host in the folder:

  - To delete the specified host, click **Yes**.
  - To delete all hosts and subfolders in the selected folder, without further prompts, click **Yes to All**.
    - To cancel the deletion, click **No**.
    - To cancel any further deletion of hosts in the selected folder, and leave the remaining contents intact, click **Cancel**.

The NMC server deletes non-unique hosts, and folders containing only non-unique hosts without additional prompting.

**NOTICE**

If there are user group restrictions in place that control which hosts a user can view, the folder might appear empty.

---

## Copying a folder

### Procedure

1. From the **Console** window, click **Enterprise**.
2. Right-click the folder to copy, then select **Copy**.
3. Right-click a new location, then select **Paste**. A copy of the folder appears in its new location.

**NOTICE**

You can also use the drag-and-drop feature to copy folders while holding down the Ctrl key.

---

4. A folder cannot be copied within the same Enterprise level.

## Moving a folder

### Procedure

1. From the **Console** window, click **Enterprise**.
2. Right-click the folder to move, then select **Move**.
3. Right-click a new location, then select **Paste**. The folder appears in its new location.

**NOTICE**

You can also use the drag-and-drop feature to move folders while holding down the Ctrl key.

---

## Renaming a folder

### Procedure

1. From the **Console** window, click **Enterprise**.
2. Right-click the folder, then select **Rename**.
3. Highlight the folder name and type a new name to replace it. The name must meet these criteria:

- Include at least one, but no more than 80 characters.
  - Exclude forward slashes (/).
4. Press **Enter**.

## Adding or deleting multiple servers by using a hostname file

For larger enterprises, use the `gstmodconf` command and a hostname file to add or delete multiple NetWorker servers to the Enterprise, with the features Capture Events and Gather Reporting Data enabled. [Using the `gstmodconf` command on page 485](#) provides more information about the `gstmodconf` command.

### Restrictions

Before you use the `gstmodconf` command, review the following restrictions.

If a host already exists anywhere in the Enterprise (either at the base or within a folder), you cannot use the `gstmodconf` command to add copies of the host.

You cannot use this command to add a host to a folder. You can only add a host to the base level of the Enterprise. After you add the host to the Enterprise, use the Console GUI to move the host to a folder. [Moving a host on page 483](#) provides more information.

When you use the `gstmodconf` command to delete a host, the command only deletes hosts from the base level. The command does not delete hosts that are within folders.

### Creating the hostname file

To use the `gstmodconf` command to add or delete multiple hosts at the same time, specify the hostnames in a hostname text file.

To create a hostname file, use these guidelines.

- Only list one hostname on each line of the file.
- A non-comment line that contains more than one space-separated or tab-separated hostname generates an error.
- To include a comment in the file, start the line with a "#" character.
- Blank lines are treated as comments and ignored, as shown in the following example.

```
Hostname file
#This is a hostname file for XYZ Corporation
apple
banana
grape
kiwi
mango
nectarine
pineapple
strawberry
tangerine
```

### Using the `gstmodconf` command

The `gstmodconf` command has this syntax:

```
gstmodconf -i file -f function -s server -k -p port -l username -P password
```

The *EMC NetWorker Command Reference Guide* or the UNIX man pages provide a complete description of the command and its options.

The following provides an example of how to use `gstmodconf` to add nodes from the file, `xyz_hostlist`. In this example, the NMC server name is `myconsole` and the `xyz_hostlist` file contains the following entries:

```
apple
banan
grape
```

#### Example: Adding multiple hosts with the `gstmodconf` command

```
% gstmodconf -s myconsole -i xyz_hostlist
Trying 111.22.3.444... connected
processing file'xyz_hostlist'
adding host 'apple'
successfully added host 'apple'
adding host 'banana'
successfully added host 'banana'
adding host 'grape'
successfully added host 'grape'
//Closing connection
```

#### Error messages generated by the `gstmodconf` command

This section describes two common error messages that can appear when you use the `gstmodconf` command.

The following provides an example of the error that appears when you use the `gstmodconf` command to add a host that already exists in the Enterprise:

#### Example: You attempt to add a host that already exists

```
% gstmodconf -s myconsole -i xyz_hostlist
Trying 111.22.3.444... connected
processing file 'xyz_hostlist'
adding host 'apple'
//Error!
{
    string object_type = "gterror";
    int severity = 16;
    int reason = 23;
    list msg = {
        int level = 1;
        string text = 'Host name already exists';
    };
// Closing connection...
```

The following output provides an example of the error that appears when you use the `gstmodconf` command but you did not specify the administrator password when the password is not the default value.

#### Example: Attempting to use `gstmodconf` without specifying the password

```
% gstmodconf -s myconsole -i xyz_hostlist
Trying 111.22.3.444... auth failed.
gt_session_connect: clnt_create: Remote system error-Connection refused.
```

## Setting up the server

When you set up the NetWorker server, enter the NetWorker product serial number that appears on the Enabler Certificate that you received from EMC Licensing.

### Procedure

1. From the **Administration** window, click **Configuration**.
2. Select the server name.
3. From the **File** menu, select **Properties**.
4. In the **Properties** dialog box, configure the appropriate attributes.
5. Click the **System Summary** tab and enter the product serial number for the server, as well as any other required information.
6. Click **Ok**.

## License the NetWorker server

The *EMC NetWorker Licensing Guide* describes how to license the NetWorker server.

## Setting the Job inactivity timeout

Use the Job inactivity timeout attribute to specify the maximum time, in minutes that the NetWorker server should wait for a response from a job before the server considers the job inactive and terminates the job.

The job activity timeout applies to all processes throughout the entire runtime operation and differs from the savegrp inactivity timeout. The savegrp inactivity timeout only applies to save processes during a media session.

### Procedure

1. On the **Administration** window, click **Configuration**.
2. In the left pane of the **Configuration** window, select the NetWorker server.
3. From the **File** menu, select **Properties**.
4. Select the **Configuration** tab.
5. In the **Job inactivity timeout** attribute, specify the timeout value in minutes.
6. Click **Ok**.

## Hostname changes

NetWorker considers each unique client name as a separate client. NetWorker assigns each unique client name in the datazone a unique identifier called a client ID. NetWorker stores the client ID for each client in the media database.

The NetWorker software has a built-in mechanism to prevent the `nsrld` daemon from starting on the NetWorker server if the startup process detects a change in the name of the NetWorker server. For example, when you change the hostname of the NetWorker server or modify the aliases order in the `hosts` file.

A message similar to the following appears in the `daemon.raw` file:

NetWorker is unable to continue its startup sequence due to a server hostname change to `hostname`. Please verify that the server's hostname

and its aliases are properly represented in the local host database (eg. /etc/hosts) and DNS.

This mechanism prevents the NetWorker software from assigning a new client ID to the NetWorker server, based on the new hostname. To resolve this issue, verify the hostname resolution of the NetWorker server. The Networking and Connectivity chapter provides more information.

If the startup process did not detect the hostname change, NetWorker will assign the NetWorker server a new client ID, which can impact NetWorker operations. To resolve this issue, use the `nsrclientfix` command to analyze the media database and identify client ID inconsistencies. You can also use the `nsrclientfix` command to merge information about multiple clients in the media database and resource database into one client resource with the original client ID. KB article 000185727 on the [EMC Support website](#) describes how to use the `nsrclientfix` command to identify and correct client ID inconsistencies.

#### Note

The SolVe Desktop application describes how to rename a NetWorker server.

## Report home

The installation of the NetWorker server software enables report home feature by default. Report home requires email capability on the NetWorker server. This connection enables the delivery of NetWorker configuration information to EMC Support when an event in the NetWorker software triggers a default notification.

The default notification sends an email that includes the NSR RAP attribute data to EMC Support. The email does not include other information or client data.

On windows, the default path for the report home output file is located in:

`NetWorker_install_path\nsr\applogs\rh`

## Enabling the report home feature

To enable the report home feature, use the `nsradmin` interface to specify an mail server that supports SMTP relay.

#### Procedure

- From the NetWorker server, start the `nsradmin` program:

`nsradmin`

- At the `nsradmin` prompt, type:

`print type: nsr report home`

- Edit the mail program attribute of the report home resource and type the name of the default mail server. For example, type:

`update mail program: smtpmail -h mailserver`

- To review the resource configuration, type:

`print`

5. To quit the nsradmin. program, type:

```
quit
```

## Manually running a report home report

To configure a report home report to start immediately and run outside of the scheduled time, use the nsradmin interface.

### Procedure

1. On the NetWorker server, start the nsradmin program from a command prompt.
2. At the nsradmin prompt, type:

```
print type: NSR task; name: DefaultReportHomeTask
```

3. To edit the **autostart** attribute of the **DefaultReportHomeTask** resource and set it to **start now**, type:

```
update autostart: start now
```

4. To review the resource configuration, type:

```
print
```

5. To quit the nsradmin program, type:

```
quit
```

## Disabling the report home feature

To disable the report home feature, use the nsradmin interface .

### Procedure

1. On the NetWorker server, start the nsradmin program from a command prompt.
2. At the nsradmin prompt, type:

```
print type: NSR task; name: DefaultReportHomeTask
```

3. To edit the **autostart** attribute of the **DefaultReportHomeTask** resource and set it to **Disabled**, type:

```
update autostart: Disabled
```

4. To review the resource configuration, type:

```
print
```

5. To quit the nsradmin program, type:

```
quit
```

## Specifying additional email recipients for the report home report

You can modify the additional email address attribute to include any internal company email address. You can use this feature to test that emails are correctly being sent.

### Procedure

1. On the NetWorker server, start the nsradmin program from a command prompt.

2. At the nsradmin prompt, type:

```
print type: nsr report home
```

3. To edit the **additional email recipients** attribute and specify additional email recipients, type:

```
update additional email recipients: my_email@address.com
```

4. To review the resource configuration, type:

```
print
```

5. To quit the nsradmin. program, type:

```
quit
```

## Specifying the sender email address

You can edit the sender email address attribute to include any internal company email address.

### Procedure

1. From the NetWorker server, start the nsradmin program:

```
nsradmin
```

2. At the nsradmin prompt, type:

```
print type: nsr report home
```

3. Edit the **sender email address** attribute and type the additional email recipients. For example, type:

```
update sender email address: my_email@address.com
```

4. To review the resource configuration, type:

```
print
```

5. To quit the nsradmin. program, type:

```
quit
```

## Parallelism and multiplexing

Parallelism is a general term within the NetWorker software for a number of configurable options that allow you to adjust the volume of data that a system processes, which can improve the performance of servers, storage nodes, and devices. Multiplexing is the ability to write multiple save streams simultaneously to the same storage device.

This section identifies attributes related to parallelism and multiplexing and describes how they work together to optimize your NetWorker environment.

### Parallelism

You can use several attributes in various NetWorker resources to adjust the volume of data that a system processes to improve overall performance.

The following attributes are related to parallelism:

- Client parallelism
- Server parallelism

- Savegrp parallelism
- Max active devices
- Media library parallelism

These attributes are described in detail in the following sections.

## Client parallelism

Client parallelism defines the number of save streams that a client can send simultaneously during backup.

Client parallelism has two default values, depending on whether the Client resource is a NetWorker server:

- For the client resource of the NetWorker server, the default value for the client parallelism attribute is 12. This higher default value allows the server to complete a larger number of index backups while during a file system backup of the server or other index backups.
- For all other clients the default value is 4. [Creating and configuring the NDMP client resource on page 569](#) provides more information about recommended parallelism settings for NDMP clients.

To define client parallelism, use the Parallelism attribute of the Client resource. You can find the parallelism attribute on the Globals(1 of 2) tab of the Client property dialog box, in the **NetWorker Administration** window.

To avoid disk contention for all clients that are not the NetWorker server, do not set the client parallelism higher than the number of physical disks involved that you configure the client resource to back up in the client's backup. For a Windows client with the ALL keyword save set attribute, the backup includes the local disks, for example C: and D: drives as well as the System State and System DB. In this example, you can keep the default parallelism setting of 4. If you define multiple save sets on the same disk, for example, C:\users, C:\system, C:\docs and so on , a higher client parallelism will result in multiple save streams attempting to access the disk at the same time.

## Controlling client parallelism on virtual clients

If you are backing up virtual clients, you can base the client parallelism setting on the underlying physical host. In this way, the total number of save streams for all of the virtual clients that reside on a physical host are limited to the value specified for the physical host. For example, suppose you had ten virtual machines running on the same physical host. Each virtual machine is a NetWorker client and each client has a client parallelism of 4. This can result in a total of 40 save streams occurring on the same physical host, which would significantly slow down that system. To avoid this situation, you can specify that the client parallelism values are to be based on the underlying physical host. In this example, that would result in no more than 4 save streams occurring for the backup of the ten virtual clients.

To base virtual client parallelism values on the physical host, perform the following steps.

### Procedure

1. From the **Administration** window, click **Configuration**.
2. Select **Clients**.
3. Right-click a virtual NetWorker client resource, and then select **Properties**.
4. On the **General** tab, select the **Virtual Client** attribute and enter the name of the underlying physical host in the **Physical host** attribute.
5. On the **Globals (1 of 2)** tab, select the **Physical client parallelism** attribute.

Complete these steps for all virtual NetWorker clients that share the same physical host. Ensure that the value in the Physical host attribute is exactly the same for all virtual NetWorker client resources that share the same physical host.

## Server parallelism

To define the server parallelism for a NetWorker server, use the Parallelism attribute of the Server resource. The Parallelism attribute appears in the NetWorker Console on the Setup tab of the Server property dialog box.

Server parallelism defines the number of simultaneous save streams that the NetWorker server will allow. The default and the maximum server parallelism values vary depending on the edition of NetWorker software. Each storage node that you enable and connect to the NetWorker server can increase the parallelism maximum value. The maximum parallelism value for any NetWorker server and storage node combination can vary. The *EMC NetWorker Release Notes* provides more information.

Optimally, configure your NetWorker server to process enough save streams to keep all of the backup devices in your data zone writing at their maximum speed. When you tune the server parallelism setting, along with other settings discussed in this section, you can maximize the speed that NetWorker writes the data to backup devices.

## Savegroup parallelism

To define the savegroup parallelism value, use the Savegrp parallelism attribute of the Group resource. The Savegroup parallelism attribute appears in the NetWorker Console on the Advanced tab of the group property dialog box.

Savegroup parallelism defines the number of simultaneous save streams that a scheduled backup can generate for a NetWorker group. The default value for this attribute is 0, which means that the attribute has no effect on other parallelism settings. If the value is greater than zero, the parallelism value will override any other parallelism considerations the backups in the group would use.

Savegroup parallelism can help tune backups that involve multiple groups that overlap in their backup schedules, particularly if one group has a large number of clients. For example, if you have one group with 100 clients and another group with 4 clients, and you have the Savegrp parallelism attribute set to 0, the `savegrp` process may start as many clients in the first group as possible, up to the maximum number allowed by the server parallelism setting defined for the NetWorker server. In this scenario, the smaller group cannot start any client backups, because the server parallelism is at its maximum, and the smaller group may experience timeouts and backup failures. To avoid this situation you can set the savegroup parallelism for the larger group to a number below the server parallelism setting, which guarantees that the clients in the smaller group can start their backups.

## Max active devices

In a DDS environment, use the Max active devices attribute, on the General tab of the Storage Node resource to define the maximum number of active devices for a storage node.

This attribute sets the maximum number of devices that NetWorker may use from the storage node in a DDS configuration. In large environments with media libraries that have a large numbers of devices, it is possible that the storage node will not have the ability to optimize all of the drives in the library. The Max active devices attribute allows you to limit the number of devices that the storage node will use at a given time, which allows the storage node to have access to all of the devices in the library but does not limit the storage node to the number of devices it can fully optimize.

## Media Library parallelism

Use the Max parallelism attribute on the Configuration tab of the Library resource to define the media library parallelism.

Media library parallelism allows you to define the maximum number of available devices for inventory and label operations.

EMC recommends that you set the Max parallelism attribute of the Library resource to one less than the number of devices within the library, which allows you to reserve one device for recovery operations.

To improve the efficiency of library operations that operate on multiple volumes, use multiple devices in parallel for these operations. However, you may wish to restrict the number of devices that NetWorker uses for inventorying and labeling operations, to ensure that some devices are available for other library operations.

## Multiplexing

Multiplexing is the ability to write multiple save streams simultaneously to the same storage device. It is often more efficient for the NetWorker server to multiplex multiple save sets to the same device; there are also times when limiting the number of save streams to a particular device will improve performance of your NetWorker environment.

Use the Target sessions, Max sessions and Pool parallelism attributes to increase or limit the number of save streams that NetWorker writes to a device.

### Target sessions

Use the Target sessions attribute on the Configuration tab of the Device resource to define the optimal number of backup sessions to assign to an active device.

Target sessions is not a hard limit; to set a hard limit for the number of sessions that a particular device can accept, use the Max sessions attribute.

The Target sessions attribute aids in load balancing devices by determining when the NetWorker software should write save streams to a device.

When a save session starts, the following actions occur:

- If a device is already receiving the number of backup sessions determined by the target sessions value, the NetWorker server uses the next underutilized device for the backups.
- If all available devices are receiving the number of backup sessions determined by their target sessions value, the NetWorker server overrides the set value and uses the device with the least activity for the next backup session.

Because it is often more efficient for the NetWorker server to multiplex multiple save sets to the same device, rather than write each save set to a separate device, the NetWorker server attempts to assign to each device a number of save sets, up to the value of target sessions, before assigning a save set to another device.

### **NOTICE**

When the NetWorker software assesses how many devices need to be involved in multiple save streams assignments with the same storage node, the device with the lowest target session value is used as a reference.

## Max sessions

The Max sessions attribute on the Configuration tab of the Device resource defines the maximum number of save sessions for a device. The max sessions value is never less than the target sessions value.

## Pool parallelism

The Max parallelism attribute on the Configuration tab of the Pool resource defines the parallelism for a pool.

Pool parallelism determines the maximum number of simultaneous save streams for each device that belong to a NetWorker pool. The default value for this attribute is 0, which means that the attribute has no effect on other parallelism settings.

You can use pool parallelism to increase recovery times. For example, you can create a pool to back up business critical data and use this attribute to restrict the number of save sets that NetWorker writes in parallel to the media in the pool. As a result, recovery speed increases for data on that media.

However, when you set the Max parallelism attribute to 1, a prolonged delay between the backup of save sets may occur. To resolve this issue, increase the Max parallelism attribute for the pool resource.

### Note

For AFTD and DD Boost devices, the Max nsrmmmd count setting for a device affects the Max parallelism attribute. For example, consider an AFTD device (AFTD\_1) that has a Max sessions attribute of 20 and a Max nsrmmmd count of 4. Now suppose a backup pool with a Pool parallelism attribute of 1 selects AFTD\_1. The total number of save sessions that NetWorker can initiate for AFTD\_1 is 4, one for each nsrmmmd process. Tape and FTD devices can only spawn one nsrmmmd process at a time, so if the previous example used a tape device, then the total number of save sessions would be 1.

## Managing server access

User privileges define the NetWorker operations and tasks that NMC, AD, and LDAP users can perform on a NetWorker server.

The *EMC NetWorker Security Configuration Guide* describes how to restrict access to the NetWorker server and NetWorker operations, including the following information:

- How to restrict administrator access to the NetWorker server.
- How to modify the privileges assigned to NMC, LDAP, and AD users and groups.
- How to Restrict server and client initiated backup and recover operations.

## Working with the Multi-Tenancy Facility

Use the Multi-Tenancy Facility option to create multiple restricted data zones. End users can access a single NetWorker server without being able to view data, backups, recoveries, or modify configurations in other data zones. In addition, Tenant administrators within a restricted data zone can only see a very limited amount of the information (log and alerts) managed by the global administrator or other restricted data zones from the Console or the CLI.

To enable the Multi-Tenancy Facility feature, configure a Restricted Data Zone resource on the NetWorker server. A restricted data zone is associated with its own NetWorker

resources. The *EMC NetWorker 8.0 Release Notes* provides information about NetWorker Module support within a restricted data zone.

## Users within a restricted data zone

The following roles apply to the Multi-Tenancy Facility feature:

- global administrator
- tenant administrator

### Global administrator

A global administrator oversees several restricted data zones to ensure the proper setup and use of the restricted data zone, and to resolve issues that the tenant administrators cannot resolve by themselves.

A global administrator for a restricted data zone requires the following configuration:

- A member of the Administrator list in the NetWorker Server Properties window of the NetWorker server. [Managing server access on page 494](#) provides more information.
- The following NetWorker software access rights:
  - The Console User role, if the global administrator requires access to NMC.
  - Either of the following privileges on the NetWorker server:
    - Configure NetWorker, which includes the following privileges:
      - Operate NetWorker
      - Monitor NetWorker
      - Operate Devices and Jukeboxes
      - Backup Local Data
      - Recovery Local Data
    - Create Application Settings, which includes the following privileges:
      - View Application Settings
      - Change Application Settings
      - Delete Application Settings

### Tenant administrator

A tenant administrator can only manage backups and recoveries within a restricted data zone. Tenant administrators can create, view, operate, manage, and modify the NetWorker resources within their own restricted data zone; not the restricted data zones of other tenants.

#### NOTICE

A tenant administrator cannot create or edit a Restricted Data Zone resource but a tenant administrator can view the resource from the Console or the CLI.

---

The procedures to configure a tenant administrator differ for native NMC authentication and LDAP/AD authentication.

## Considerations

When configuring tenant administrators within the restricted data zone, consider the following information.

- Non-default resources in the global data zone are not visible to tenant administrators who only have privileges within the restricted data zone.
- Tenant administrators cannot be a member of more than one unique restricted data zone. However, a tenant administrator can appear in multiple resource instances of the same restricted data zone. This allows for fine grain control over the tenant administrator and their privileges because all restricted data zones group together in a similar way that Client resources with the same name group together. [Configure multiple Restricted Data Zones resources that use the same name on page 508](#) provides details.
- A restricted data zone can have multiple tenant administrators.
- The Privileges section of the Restricted Data Zone resource specifies the privileges for a tenant administrator.  
For resources that have a restricted data zone associated with them, the Restricted Data Zone resource and the User Groups resource use the same Privileges attributes.
- Tenant administrators can only create devices and jukeboxes on storage nodes that are associated to them exclusively within the restricted data zone.

**NOTICE**

Do not use the wild card character \* in the Users attribute of a Restricted Data Zone resource.

### Creating a tenant administrator when using native authentication

The global administrator configures a restricted data zone and assigns tenant administrators.

[Configuring a restricted data zone on page 499](#) describes how to configure a restricted data zone and add a tenant administrator to the restricted data zone.

### Procedure

1. (Optional) Create the Console user create a Console user account if access to NMC is required.

To create a Console user account:

- a. Log in to the Console server as a Console Security Administrator.
- b. From the **Console** window, click **Setup**.
- c. In the left pane, right-click **Users** and select **New**. The **Create User** dialog box opens and displays the **General** tab.
- d. In the **User Name** field, type a username for the tenant administrator. The username must not:
  - Exceed 20 characters.
  - Use spaces or any of these characters:  
— :  
— <>  
— /
  - Use characters with an ASCII value less than or equal to 32.
  - Begin a username with an underscore (\_) character.

- e. (Optional) In the **Full Name** field, type the full name of the user.
  - f. (Optional) In the **Description** field, type the user description.
  - g. In the **Role** field, select **Console User**.
  - h. In the **Password** field, type the user password for the tenant administrator.  
Passwords must be at least eight characters long and cannot be the same as the user name. The Console server enforces this requirement when you create or edit users or when you change a user password after you upgrade from a previous release.
  - i. In the **Confirm Password** field, retype the password and click **OK**.  
If records are enabled, all Console users can query records.
2. Add the Console user account that you created or other user account to the **Users** field in the Restricted Data Zone resource.
3. Assign privileges to the tenant administrator within the restricted data zone.
- Creating a tenant administrator when using LDAP authentication**  
The global administrator configures a restricted data zone and assigns tenant administrators.
- When an LDAP user logs in for the first time, a user object is automatically created on the Console server. You only need to map LDAP user roles or LDAP user names to Console user roles. If necessary, you can also create user objects before users log in for the first time. For example, you may want to restrict user access to managed servers before the user logs in for the first time.
- EMC NetWorker Security Configuration Guide describes how to configure NMC and the NetWorker software into LDAP mode.
- Procedure**
1. (Optional) Create the Console user:
    - a. Log in to the Console server as a Console Security Administrator.
    - b. From the **Console** window, click **Setup**.
    - c. In the left pane, right-click **Users** and select **New**. The **Create User** dialog box opens and displays the **Identity** tab.
    - d. In the **User Name** attribute, type the LDAP user name.
    - e. Optional) In the **Full Name** field, type the full name of the LDAP user.
    - f. (Optional) In the **Description** field, type the user description.
    - g. Click **OK**.
  2. Map LDAP users to Console roles.
    - a. In the left pane, select **Roles**.
    - b. In the right pane, right-click **Console User** and select **Properties**.
    - c. In the **External Roles** attribute, add each LDAP user role or LDAP user name to be mapped. Type each entry on a separate line.
  3. Click **OK**.
  4. Assign privileges to the tenant administrator within the restricted data zone.

## Create reports for a Restricted Data Zone

NetWorker allows global administrators to generate NMC reports for all restricted data zones on each NetWorker server that the NMC server manages.

A tenant administrator can generate reports for an RDZ under the following conditions:

- The tenant administrator has access to the RDZ.
- The tenant administrator only has access to the NetWorker servers that include the RDZs this user has permission to access. To restrict the NetWorker servers that a tenant administrator has permission to access, edit the managed server list for the user account:
  1. From the **Console** window, select **Setup**.
  2. In the left pane, click **Users**.
  3. Right-click a user account and select **Permissions**.
  4. Modify the **Managed host** field to contain only the NetWorker servers you want the user to access.
  5. Click **OK**.

---

### Note

The Restricting managed server view for a user section in the *EMC NetWorker Security Configuration Guide* provides more information about the implications that result when you restrict a view for a user.

---

When a tenant administrator has access to multiple RDZs on different NetWorker servers, the reporting feature will work as expected only when you use the same name for the RDZ on each NetWorker server.

## View data within a Restricted Data Zone

To aid in the segregation of restricted data zones, some resources have limited visibility. Tenant administrators within a restricted data zone cannot view or modify the resources of other third-party restricted data zones. Resources and save set information do not appear to a tenant administrator, who is outside of a restricted data zone.

Tenant administrators can view some resources, but cannot associate them with a restricted data zone. This allows some of the basic functionality of the NetWorker software to be performed.

Only the default pre-sets of the following NetWorker resources are always visible to the tenant administrator within the restricted data zone:

- Directives
- Label Templates
- Media Pools
- Schedules
- Policies

For example, the Encryption directive is always visible to all restricted data zones.

Tenant administrators see a limited view of NetWorker resources. When tenant administrators review their own restricted data zone, the list of selectable resources is limited to the resources that the global administrator specified for them in the Restricted

Data Zone resource. Tenant administrators can perform report queries to view basic information about clients and save sets. File data is not available.

## Restricted Data Zone resource associations

When tenant administrators create a new resource, providing that they have permission to do so, that new resource is automatically associated to their restricted data zone.

When the resource is created, the restricted data zone's restriction counts are checked. An error message appears if the restriction count is exceeded.

When a global administrator or a tenant administrator deletes a resource from the restricted zone, the resource is automatically disassociated from its original restricted data zone.

For resources that exist in multiple instances such as clients, when you delete the last copy of the resource, the Restricted Data Zone resource disassociates. You can manually disassociate resources by deleting the original resource.

### Special case associations

Associations between the following resources have a special built-in inheritance policy:

- Groups and clients
- Jukeboxes and devices

If a group or jukebox is associated or disassociated to a restricted data zone, then all of its related clients or devices are associated or disassociated when a change to the resource is committed. This function ensures that resources are not partially associated to a restricted data zone.

## Configuring a restricted data zone

To configure a restricted data zone, you apply a set of privileges on a per resource basis. Note that you apply User Groups privileges on a per data zone level.

The association of a restricted data zone to resource is one-to-many, such that a restricted data zone can be associated with multiple resources. However, a single resource can not be associated to different restricted data zones. When a resource is associated to a restricted data zone, it is immediately made available for use by the restricted data zone.

### Note

NetWorker clients and groups that are associated to a restricted data zone must both belong exclusively to that particular restricted data zone, and must not participate in other restricted data zones. The Multi-Tenancy Facility feature does not support a scenario where one group is used to back up clients that belong to different restricted data zones.

Error messages appear if there is an attempt to:

- Associate more of a particular type of resource than is specified in the Restriction attribute of the Restricted Data Zone resource.
- Configure a resource which cannot be associated to a Restricted Data Zone.

Tenant administrators cannot create or edit a Restricted Data Zone resource. However, they can view the resource from the Console or CLI.

To configure a restricted data zone, you must create or edit a Restricted Data Zone resource.

### Procedure

1. Ensure that you have at least the minimum privileges to create or edit a Restricted Data Zone resource. [Global administrator on page 495](#) provides more information about required privileges.
2. To configure a restricted data zone where tenant administrators are assigned:
  - a. Ensure that the tenant administrators are not listed in **Users** attribute of any User Groups resources. Privileges set in a User Groups resource apply to all resources, not just the resources within a Restricted Data Zone.  
Privileges that are set for the tenant administrator apply to all resources within the restricted data zone.
  - b. Remove the \*@\* character from the **Users** attribute of each of the NetWorker User Groups resources. By default, \*@\* appears in the **Users** field of the User Groups resource named Users.  
If the \*@\* characters are left in the access attribute of any NetWorker User Group resource or in the Remote Access attribute of any NetWorker resource such as a Client resource, then that resource will be visible from any restricted datazone.
3. Configure the following customized NetWorker resources for the restricted data zone, if required.

Default directives, labels, media pools, schedules, and policies are available to all restricted data zones at all times:

- Groups — A backup group specifies the time of day when a backup occurs. [Backup Groups and Schedules on page 243](#) provides information about groups.  
NetWorker groups and clients that are associated to a restricted data zone must both belong exclusively to that particular restricted data zone, and must not participate in other restricted data zones. The Multi-Tenancy Facility feature does not support a scenario where one group is used to back up clients that belong to different restricted data zones.
- Directives — Optional instructions that control how files and directories are processed during backup and recovery. [Preconfigured global directive resources on page 274](#) provides more information about the preconfigured directive options.
- Labels — If you are not using tapes with barcode labels, and the Match Bar Code Labels attribute is not enabled for the Library resource, then every backup volume requires a unique label for identification. The NetWorker server creates a unique label for each volume by applying a label template. [Label templates on page 298](#) provides more information about the preconfigured label templates.
- Media Pools — A collection of volumes to which backup data is written. Pools are used to sort backup volumes so that the volumes are easy to locate when they are required. [Media pools on page 284](#) provides more information about media pools.
- Schedules — The NetWorker software ships with preconfigured schedules. If these schedules meet backup requirements, use them as is. Otherwise, create new schedules to accommodate any site-specific requirements. [Schedules on page 256](#) provides more information about schedules.
- Policies — Specifies a time range that the Restricted Data Zone resource takes effect. You can use the Policies resource to create or modify the preconfigured policies. [Preconfigured time policies on page 238](#) provides more information about policies.

4. In the server Administration interface, click Configuration.

5. Right-click **Restricted Data Zones** and select **New**. The **Create Restricted Data Zone** dialog box appears.
6. On the **General** tab, in the **Name** field, type the name of the restricted data zone.
7. (Optional) In the **Comment** field, add a descriptive comment for the restricted data zone.
8. On the **General** tab, set restrictions to limit the number of clients, devices, storage nodes, and jukeboxes that the tenant administrator can create or associate within the restricted data zone:
  - a. In the **Number of clients** field, set restrictions to limit the number of clients that the tenant administrator can create or associate within the restricted data zone.
  - b. In the **Number of devices** field, set restrictions to limit the number of devices that the tenant administrator can create or use within the restricted data zone.
  - c. In the **Number of storage nodes** field, set restrictions to limit the number of storage nodes that the tenant administrator can create or associate to the restricted data zone.
  - d. In the **Number of jukeboxes** field, set restrictions to limit the number of jukeboxes that the tenant administrator can create or use within the restricted data zone.

You must use AlphaStor when two restricted data zones share a jukebox.

9. List the tenant administrators and assign their privileges within the restricted data zone:
  - a. Add the user accounts that are granted permission to create and manage the NetWorker resources within this particular restricted data zone.

The procedures differ for native authentication and LDAP/AD authentication:

- For LDAP authentication:
  - a. In the **External roles** field, add the user accounts that are granted permission to create and manage the NetWorker resources within this particular restricted data zone as a tenant administrator.
  - b. Leave the **Users** field blank.
- For native authentication, in the **Users** field, add the user accounts that are granted permission to create and manage the NetWorker resources within the particular restricted data zone as a tenant administrator.

Use the following format:

```
sam@jupiter or user=sam, host=jupiter - User Sam on machine
jupiter
host=jupiter - Any user on machine jupiter
```

Tenant administrators that appear in the **Users** field can only create the NetWorker resources within their particular restricted data zone; not the restricted data zones of other third party users. [View data within a Restricted Data Zone on page 498](#) provides more information.

- b. In the **Privileges** field, select the privileges that are required for the tenant administrators to create and manage resources within this particular restricted data zone. [Customizing privileges on page 503](#) provides more information.

---

**Note**

Privileges you set for the tenant administrator apply to all resources within the restricted data zone.

---

10.In the **Group and Clients** tab:

- a. Select the groups that the specified tenant administrator can access within this particular restricted data zone. A backup group specifies the time of day when a backup occurs. [Backup Groups and Schedules on page 243](#) provides information about groups.

The group must only contain NetWorker clients that belong exclusively to that particular group.

If a group is associated or disassociated to a restricted data zone, then all of its related clients are associated or disassociated automatically when a change to the resource is committed. This setting ensures that resources are not partially associated to a restricted data zone.

- b. Select the clients that can be administered by the specified users within this particular restricted data zone.

A client that belongs to a group must be associated with a restricted data zone. If a client is not associated with a restricted data zone, then the client is considered to belong to the global data zone and is not considered to be part of the restricted data zone.

---

**Note**

NetWorker groups and clients that are associated to a restricted data zone must both belong exclusively to that particular restricted data zone, and must not participate in other restricted data zones. The Multi-Tenancy Facility feature does not support a scenario where one group is used to back up clients that belong to different restricted data zones.

---

11.In the **Jukeboxes and Devices** tab:

- a. Select a jukebox that the specified tenant administrator can access within this particular restricted data zone.
- b. Select a device that the specified tenant administrator can access within this particular restricted data zone.

**NOTICE**

If a jukebox is associated or disassociated to a restricted data zone, then all of its related devices are associated or disassociated when you save the change to the resource. This setting ensures that resources are not partially associated to a restricted data zone.

---

A global administrator can share storage nodes by assigning devices and jukeboxes on a storage node to multiple restricted data zones. However, the storage nodes are not marked as associated in the Restricted Data Zone resource. [Associate storage nodes to the restricted datazone on page 507](#) provides more information.

A tenant administrator can only create devices and jukeboxes on storage nodes that are associated to them exclusively in the restricted data zone by the global administrator.

12.If required, select the already configured customized NetWorker resources that you configured for the restricted data zone:

- In the **Directives** tab, select a directive that can be accessed and used by the specified tenant administrator within this particular restricted data zone. Directives are optional instructions that control how files and directories are processed during backup and recovery. [Preconfigured global directive resources on page 274](#) provides detailed information about the preconfigured directive options.

**NOTICE**

Default directives, labels, media pools, schedules, and policies are available to all restricted data zones at all times.

- In the **Labels** tab, select labels for the backup volumes. The tenant administrators within the restricted data zone can access these volumes. [Label templates on page 298](#) provides more information about the preconfigured label templates.
- In the **Media Pools** tab, select the media pools that can be accessed and used by the specified tenant administrators within this particular restricted data zone. Media pools are a collection of volumes to which backup data is written. Pools are used to sort backup volumes so that the volumes are easy to locate when they are required. [Media pools on page 284](#) provides detailed information.
- In the **Schedules** tab, select a schedule that can be accessed and used by the specified tenant administrators within this particular restricted data zone. [Schedules on page 256](#) provides detailed information.
- In the **Policies** tab, select a policy to specify a time range that the restricted data zone resource takes effect. You can use the Policies resource to create or modify the preconfigured policies. [Preconfigured time policies on page 238](#) provides more information.

13.On the **Storage Nodes** tab, select a storage node that the tenant administrator can access and use within the restricted data zone:

- A global administrator can share storage nodes by assigning devices and jukeboxes to multiple restricted data zones. However, the storage nodes are not marked as associated in the Restricted Data Zone resource. [Associate storage nodes to the restricted datazone on page 507](#) provides more information.
- A tenant administrator within a restricted data zone can only create devices and jukeboxes on storage nodes that are associated to their restricted data zone.

14.In the **Operation Status** tab, do not change the default setting.

NetWorker sets the Operation Status automatically and you cannot manually associate the status to a restricted data zone.

15.Click **Ok** to complete the configuration. You can view the newly created restricted data zone in the **Restricted Data Zone** pane.

## Customizing privileges

You can customize privileges associated with a tenant administrator within a restricted data zone to fit specific requirements. You can assign the tenant administrator privileges in the Privileges field of the Restricted Data Zone resource.

The following table provides a list of the preconfigured privileges and their associated privileges.

**Table 92** Tenant administrator privileges

| Privilege                 | Privileges                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |
|---------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Remote Access All Clients | <p>Allows a tenant administrator to:</p> <ul style="list-style-type: none"> <li>• Remotely browse and recover data associated with any client within the restricted data zone.</li> <li>• View configurations for all Client resources that are within the restricted data zone.</li> </ul> <p>This privilege is required to perform Directed Recovers. This privilege supersedes the Remote Access attribute in the Client resource.</p> <p>You must also enable the following five privileges:</p> <ul style="list-style-type: none"> <li>• Operate NetWorker</li> <li>• Monitor NetWorker</li> <li>• Operate Devices and Jukeboxes</li> <li>• Backup Local Data</li> <li>• Recover Local Data</li> </ul> |
| Operate NetWorker         | <p>Allows a tenant administrator to perform NetWorker operations. For example, members can perform the following tasks with their restricted data zone:</p> <ul style="list-style-type: none"> <li>• Reclaim space in a client file index.</li> <li>• Set a volume location or mode.</li> <li>• Start or stop a savegroup.</li> <li>• Query the media database and client file indexes.</li> </ul> <p>You must also enable the following five privileges:</p> <ul style="list-style-type: none"> <li>• Monitor NetWorker</li> <li>• Operate Devices and Jukeboxes</li> <li>• Backup Local Data</li> <li>• Recover Local Data</li> </ul>                                                                     |
| Configure NetWorker       | <p>Allows a tenant administrator to configure the following resources associated with the NetWorker server, its storage nodes, and clients. This includes creating, editing, and deleting resources within the restricted data zone:</p> <ul style="list-style-type: none"> <li>• Clients</li> <li>• Devices</li> <li>• Directives</li> <li>• Groups</li> <li>• Jukeboxes</li> <li>• Labels</li> <li>• Media Pools</li> <li>• Policies</li> <li>• Schedules</li> <li>• Storage Nodes</li> </ul> <p>You must also enable the following five privileges:</p>                                                                                                                                                  |

**Table 92** Tenant administrator privileges (continued)

| Privilege                     | Privileges                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |
|-------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|                               | <ul style="list-style-type: none"> <li>• Operate NetWorker</li> <li>• Monitor NetWorker</li> <li>• Operate Devices and Jukeboxes</li> <li>• Backup Local Data</li> <li>• Recover Local Data</li> </ul> <p>Tenant administrators can only edit resources within their own particular restricted data zone. However, they can create new resources if they are not blocked by the quantity restrictions in the Restricted Data Zones resource.</p> <p>Tenant administrators with this privilege can not configure NetWorker resources that have not been assigned to them within the restricted data zone.</p> <p>Tenant administrators can not configure the following resources:</p> <ul style="list-style-type: none"> <li>• User Group resource</li> <li>• Restricted Data Zone resource</li> </ul> <p>Tenant administrators with this privilege can not enable the Remote Access attribute in the Client resource. Permission to change the Remote Access attribute in the Client resource is granted only through the Change Security Settings privilege.</p> |
| Monitor NetWorker             | <p>Allows a tenant administrator to:</p> <ul style="list-style-type: none"> <li>• Monitor NetWorker operations, including device status, save group status, and messages.</li> <li>• View media databases information.</li> <li>• View NetWorker configuration information within the restricted data zone.</li> </ul> <p>This privilege is not required to back up and recover local data. However, this privilege might be helpful for a tenant administrator to monitor messages and other information.</p> <p>While most information is limited to what is within the restricted data zone. A tenant administrator with this privilege can view all of the current log messages and alerts that are present in the NetWorker software by using NMC or the nsrwatch command.</p>                                                                                                                                                                                                                                                                               |
| Operate Devices and Jukeboxes | <p>Allows a tenant administrator to perform device and autochanger operations within the restricted data zone. For example, operations such as mounting, unmounting, and labeling.</p> <p>You must also enable the Monitor NetWorker privilege.</p> <p>A tenant administrator with this privilege can also view device status, and pending messages, and view information in the media database.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              |
| Recover Local Data            | <p>Allows a tenant administrator to recover data from the NetWorker server to the local client and to view most attributes in the client's configuration.</p> <p>This privilege does not provide permission to view information about other clients.</p> <p>This privilege does not override file-based privileges. Tenant administrators can only recover files with the appropriate user privileges for the operating system.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |

**Table 92** Tenant administrator privileges (continued)

| Privilege                   | Privileges                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |
|-----------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|                             | A tenant administrator with this privilege still must log in as root (UNIX) or administrator (Microsoft Windows) to perform save set or NDMP recoveries.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |
| Backup Local Data           | Allows a tenant administrator to manually back up data from local clients in the restricted data zone to the NetWorker server. Use the nsradm command to query information about the current client backup.<br>This privilege does not override file-based privileges. A tenant administrator can only back up files with the appropriate user privileges for the operating system. A tenant administrator with this privilege still must log in as root (UNIX) or administrator (Microsoft Windows) to run the savegrp command or perform NDMP backups.<br>To allow scheduled backups to operate correctly, the root user (UNIX) or administrator (Microsoft Windows) on the client has this privilege by default. |
| Archive Data                | This privilege has no effect in a restricted data zone.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             |
| Backup Remote Data          | This privilege has no effect in a restricted data zone.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             |
| Recover Remote Data         | This privilege has no effect in a restricted data zone.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             |
| Delete Application Settings | Allows a tenant administrator to delete application settings that were set in the NetWorker software for the particular data zone.<br>You must also enable the following three privileges: <ul style="list-style-type: none"><li>• Create Application Settings</li><li>• View Application Settings</li><li>• Change Application Settings</li></ul>                                                                                                                                                                                                                                                                                                                                                                  |
| Change Application Settings | Allows a tenant administrator to change application settings that were set in the NetWorker software for the particular data zone.<br>You must also enable the following three privileges: <ul style="list-style-type: none"><li>• Create Application Settings</li><li>• View Application Settings</li><li>• Delete Application Settings</li></ul>                                                                                                                                                                                                                                                                                                                                                                  |
| View Application Settings   | Allows a tenant administrator to view application settings that were set in the NetWorker software for their particular data zone.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |
| Create Application Settings | Allows a tenant administrator to create application settings for their particular data zone.<br>You must also enable the following three privileges: <ul style="list-style-type: none"><li>• View Application Settings</li><li>• Change Application Settings</li><li>• Delete Application Settings</li></ul>                                                                                                                                                                                                                                                                                                                                                                                                        |
| Change Security Settings    | Allows a tenant administrator to edit the Remote Access attribute in the Client resources that belongs to the particular restricted data zone.<br>You must also enable the following three privileges:                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              |

**Table 92** Tenant administrator privileges (continued)

| Privilege                | Privileges                                                                                                                                                                                                                                                                                                                                                                                                                       |
|--------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|                          | <ul style="list-style-type: none"> <li>• Delete Security Settings</li> <li>• Create Security Settings</li> <li>• View Security Settings</li> </ul>                                                                                                                                                                                                                                                                               |
| Delete Security Settings | <p>Prohibits a tenant administrator from deleting a security setting. Enable this privilege if you selected the Change Security Settings privilege. This privilege has no impact on the restricted data zone.</p> <p>You must also enable the following three privileges:</p> <ul style="list-style-type: none"> <li>• View Security Settings</li> <li>• Change Security Settings</li> <li>• Create Security Settings</li> </ul> |
| Create Security Settings | <p>Prohibits a tenant administrator from deleting a security setting. Enable this privilege if you selected the Change Security Settings privilege. This privilege has no impact on the restricted data zone.</p> <p>You must also enable the following three privileges:</p> <ul style="list-style-type: none"> <li>• View Security Settings</li> <li>• Change Security Settings</li> <li>• Create Security Settings</li> </ul> |
| View Security Settings   | Allows a tenant administrator to view the security settings that were set in the NetWorker software for the particular data zone.                                                                                                                                                                                                                                                                                                |

## Associate storage nodes to the restricted datazone

A global administrator can share storage nodes by assigning devices and jukeboxes to multiple restricted data zones. However, the storage nodes are not marked as associated in the Restricted Data Zone resource.

A tenant administrator within a restricted data zone can:

- Create a storage node if the global administrator has set the correct privileges and restrictions. [Customizing privileges on page 503](#) provides more information.
- Create devices and jukeboxes only on storage nodes that are associated within the restricted data zone.

You can associate storage nodes to a restricted data zone in two ways:

- Exclusive use  
For exclusive use, associate the storage node within the restricted data zone. This best practice allows tenant administrators to create their own devices and modify and delete the storage node. When a tenant administrator with the proper privilege creates a storage node, the storage node and restricted data zone automatically associate during the create process.
- Group use  
For group use, do not explicitly associate the storage node to any restricted data zone. The global administrator must create and associate devices and jukeboxes to

the restricted data zone. This allows the restricted data zones and the global data zone to all share the same storage nodes.

## Configure multiple Restricted Data Zones resources that use the same name

You can configure multiple Restricted Data Zone resources with the same name. Using one name for multiple Restricted Data Zone resources allows fine grain control over a restricted data zone's administrators and their privileges. The use of one name to group multiple Restricted Data Zone resources is similar to the way you group Client resources with the same name.

To provide optimal flexibility, you can define multiple Restricted Data Zone resources for the same data zone, with the same name.

For example, a list of restricted data zones might include two instances of a restricted data zone named Company\_One. Each instance is assigned a unique tenant administrator, each with different privileges. In this scenario, one tenant administrator is designated for configuration and the other for operation. Each tenant administrator has a different privilege set. All information in a restricted data zone, except the tenant administrators of the data zone and their privileges, are propagated to all other Restricted Data Zone resources with the same name.

You can use the Comment attribute in the Restricted Data Zone resource to help distinguish between multiple Restricted Data Zone resources with the same name.

### **NOTICE**

A tenant administrator cannot be included in more than one restricted data zone. However, a tenant administrator can be included in more than one Restricted Data Zone resource within the same restricted data zone.

## Limit the tenant administrator from creating too many resources

You can set limits on the following Restricted Data Zone resources:

- Number of clients
- Number devices
- Number of storage nodes
- Number of jukeboxes

By setting resource limits you prevent tenant administrators from overusing resources and licenses:

- If tenant administrators exceed the restriction limitations when creating or updating a resource, an error message appears notifying them that the update or creation will not be performed.
- If tenant administrators review their own restricted data zone, the list of selectable resource is limited to the resources that were specified for them in the Restricted Data Zone resource by the global administrator.

## Configurations for the Multi-Tenancy feature

The following two configurations are supported for the Multi-Tenancy Facility feature:

- A global administrator assigns tenant administrators who can create, view, operate, manage, and modify the NetWorker resources associated with their own restricted data zone; not the restricted data zones of other tenants.  
In this configuration, the global administrator sets up the initial privileges and restrictions such as the maximum numbers of clients, devices, jukeboxes, and storage nodes, and then lets the tenant administrators set up their own resources to

meet their individual business requirements. Restrictions are set in place to ensure that tenant administrators do not overuse resources, while still enabling them the freedom to set up the restricted data zone. An error message displays if the set restrictions are exceeded.

- A global administrator can manage multiple Restricted Data Zone resources. In this configuration, the global administrator controls the layout of the restricted data zones, including the set up of clients, devices, jukeboxes, storage nodes, and schedules.

## Resource databases

Information about the NetWorker server resides in series of files in the following directories:

```
NetWorker_install_path\res\nsrdb\00
.
NetWorker_install_path\res\nsrdb\09
```

NetWorker stores each resource in a separate numbered file. As you create new resources, for example, a new Client, Group, or Pool resources, the NetWorker server adds new files to the directories.

A client resource database (nsexec) also exists on each NetWorker host and contains configuration information about each NetWorker host. The nsexec database resides in the *NetWorker\_install\_path\res\nsrla.res* file

The *EMC NetWorker Security Configuration Guide* provides more information about the client resource database.

## Viewing resources in the resource database

You can view all of the NetWorker resources through the NMC Administration window.

Although you can view the contents of the new NetWorker resource files in the resource database with a text editor, EMC does not support direct user edits of the text files to modify the resources.

NetWorker provides an command line tool, nsradmin, to modify resource databases.

For example:

- To access the NetWorker server resource database, use one of the following commands:

```
nsradmin -s server_name
nsradmin -d NetWorker_install_path\res\resdb
```

---

### Note

If you inadvertently specify the wrong path with the `nsradmin -d` command, `nsradmin` creates empty resource directories. If this occurs, delete the incorrect directories.

- To access the client resource database, use the following command :

```
nsradmin -p nsexec
```

## Repairing resource database corruption

A power outage, operating system crash, or manual edits the database with a text editor can cause NetWorker resource database file corruption.

If the NetWorker server cannot read the resource files when the NetWorker services start, a message similar to following appears in the `daemon.raw` file.

```
nsrd: WARNING: NSR configuration database detected invalid
resource ...\\00019803aa14713c89456b41
nsrd: Invalid resource saved at ...\\00019803aa14713c89456b41
```

[Viewing log files on page 677](#) provides more information about viewing log files.

The NetWorker server removes any corrupt resource files from the `nsrdb` directory structure and places them in the `dbg` directory. NetWorker creates the `dbg` directory only after resource database file corruption has occurred. To correct this issue, open the corrupt file with a text editor and review the file contents, then re-create the resource. You can delete the corrupted resource file.

---

### Note

If you do not know the cause of the resource file corruption, contact Technical Support assistance.

---

## Indexes

The NetWorker server tracks the files it backs up in two databases, which are stored on the local file system of the server:

- The client file index tracks the files that belong to a save set. There is one client file index for each client.
- The media database tracks:
  - Volume name
  - Backup dates of the save sets on the volume
  - File systems in each save set
 Unlike the client file indexes, there is only one media database per server.

The client file indexes and media database can grow to become prohibitively large over time. [Managing the size of the online indexes on page 515](#) provides information about managing the size of these indexes.

## Characteristics of the online indexes

The size of an index is proportional to the number of entries the index contains. The media database is usually smaller than the client file index, because the media database stores one entry for each volume, while the client file index stores one entry for each file that NetWorker saves on a volume. The NetWorker server selects which volume to mount to perform a recovery by mapping the saved files to their volumes.

Each entry in the client file index includes this information for a saved file:

- Filename
- Number of blocks
- Access privileges

- Number of links
- Owner
- Group
- Size
- Last modified time
- Backup time

The client file indexes grow with each backup, as entries are added for each newly saved file and save set. As long as an index entry for a file remains in the client file index, you can perform a browsable recovery of the file. Over time, the size of these indexes can grow very large.

#### **NOTICE**

If the file system that contains the indexes gets full, the NetWorker server cannot access the media database and cannot recover data. Unless you use browse and retention policies to control the size of the online indexes, the indexes continue to grow until they exceed the capacity of the file system.

NetWorker uses browse and retention policies to manage the lifecycle of the data, and to automatically control the size of the client file index. [About browse and retention policies on page 232](#) provides information about policies.

## Automated index activities

The NetWorker server performs these online index activities:

- Inserts entries in the client file index for each file saved during a backup. For each new backup, the NetWorker server acquires more space from the file system for the new entries.
- Removes entries and returns disk space to the operating system. The browse and retention policies automatically determine when entries are removed from the index.

You can also remove index entries manually by clicking Remove Oldest Cycle in the Index Save Sets dialog box. [Removing the oldest save set cycles on page 517](#) provides more information.

## Checking online indexes

Each time the NetWorker server starts, the startup process uses `nsrck -ML1` to perform a level 1 consistency check on the client file indexes. In some circumstances, this consistency check will not detect corruption in the client file indexes. If you believe an index may be corrupt, run a higher level check on the index, for example:

```
nsrck -L5
```

If the index is still corrupt, recover the index by using the procedure outlined in [Recovering expired save sets on page 369](#).

EMC recommends that you periodically run the `nsrck -F` and `nsrim -X` commands to check the integrity of the client and media indexes. The *EMC NetWorker Command Reference Guide* or the UNIX man pages provide more information about these commands.

## Viewing information about the indexes

The following table identifies the index information displayed for each client.

**Table 93** Indexes window information

| Column      | Description                                                                                                                                   |
|-------------|-----------------------------------------------------------------------------------------------------------------------------------------------|
| Client Name | Names of the NetWorker clients that have been backed up by the current server.                                                                |
| Size        | Amount of disk space currently allocated to the client file index. As the index size increases, the allocated disk space automatically grows. |

### Procedure

1. From the **Administration** window, click **Media**.
2. In the left pane, click **Indexes**. The right pane displays index information for all clients of the server.

## Index save sets

The Index Save Sets dialog box displays the save sets assigned to a particular client, along with detailed information about each save set. The dialog box also includes an option to remove old save set cycles.

### Viewing client save set information

The following table identifies the information in the Save Sets dialog box for each save set.

**Table 94** Index save sets dialog box information

| Column        | Description                                                                                                                                                                                               |
|---------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Save Set Name | Name of the save set.                                                                                                                                                                                     |
| Size          | Estimated amount of the index space used by the save set in the client file index.                                                                                                                        |
| Cycles        | Number of backup cycles available for browsing. A cycle starts with a full backup and ends with the next full backup, and includes any incremental and level 1–9 backups that occur between full backups. |
| SSID          | Unique identification number of the instance of the save set.                                                                                                                                             |
| Files         | Number of files backed up during that instance.                                                                                                                                                           |
| Size          | Size of the backup.                                                                                                                                                                                       |
| Time          | Date and time of the backup.                                                                                                                                                                              |
| Level         | Level of the backup (full, incr [incremental], or 1-9)                                                                                                                                                    |

[Reduce the size of the client file index on page 516](#) provides information about reducing the size of the client file indexes by using the Remove Oldest Cycle button.

### Procedure

1. From the **Administration** window, click **Media**.

2. Click **Indexes**.
3. Right-click the client whose save sets you want to view, then click **Show Save Sets**. The **Index Save Sets** dialog box appears.
4. To view detailed information about a save set, click the save set name.

## Querying the media database

You can query the media database for information about save sets. Queries apply to all complete, browsable save sets, not just those from the last 24 hours.

### Procedure

1. From the **Administration** window, click **Media**.
2. Click **Save Sets**.
3. On the **Query Save Sets** tab, indicate the appropriate query parameters, then click the **Save Set List** tab to run the query and view the results.

**NOTICE**

If the query is unsuccessful, an error dialog box appears, which indicates that NetWorker could not find save sets that matched the specified query. Click **OK** to close the dialog box.

---

### Results

You can also use the `mminfo -av` command to query the media database. The *EMC NetWorker Command Reference Guide* or the UNIX man pages provides detailed information about how to use the `mminfo` command.

## Cross-checking client file indexes

Perform a cross-check to verify the consistency between the client file index and the media database. If the NetWorker server finds entries in the client file index that do not have corresponding entries in the media database, it removes the client file index entries. This feature is useful, for example, if you perform an index operation and the server crashes before the NetWorker server has completely updated the indexes. Once the server is running again, cross-check to accurately update the online indexes.

### Procedure

1. From the **Administration** window, click **Media**.
2. Click **Indexes**.
3. Right-click the client with the index to cross check, then select **Cross Check Index**.

The following prompt appears:

```
Cross-checking may take considerable time. Would you like to cross-
check
client_name?
```

4. Click **Yes** to continue. The NetWorker server displays a status box until the cross-checking is complete.

## Refreshing index information

Occasionally refresh the information in the Indexes tab, particularly if you are connected to a server for a long period of time.

### Procedure

1. From the **Administration** window, click **Media**.
2. Click **Indexes**.
3. From the **View** menu, select **Refresh**.

## Client file index locations

During the initial client setup, the NetWorker software normally designates a default location for the client file index on the NetWorker server. This default location is:

- For UNIX: `/nsr/index/client_name`
- For Windows: `NetWorker_install_path\index\client_name`

However, you may need to designate a different index location when first configuring a Client resource, or you might need to move the file index of an existing client. These sections address these needs.

### Designating the client file index location for a new client

#### Procedure

1. From the **Administration** window, click **Configuration**.
2. Right-click **Clients**, then select **New**. The **Create Client** dialog box appears.
3. Click the **Globals (2 of 2)** tab.
4. In the **Index Path** attribute, enter the full path of the directory where the client file index will reside.
5. For the remaining tabs, enter information as necessary to create the new client.
6. Click **Ok**.

## Changing the client file index location for an existing client

To change the client file index location to a nondefault location for an existing client, you must first move the index to its new location.

### Moving a client file index

You can move a client file index from its current location to a new location. For example, if the size of the client file index is too large, you can move it to a location with more space.

#### Procedure

1. Ensure that backups and recovers are not occurring on the NetWorker server.
2. Log in to the NetWorker server root on UNIX or as an administrator on Windows.
3. From the directory that contains the indexes, type:

```
uasm -s -i "client_index_directory_name" | (cd target_directory;
uasm -r)
```

**Note**

On Solaris and Linux platforms, `uasm` is installed in `/usr/lib/nsr`. On all other platforms, `uasm` is installed in the same location as the NetWorker binaries.

4. Use NMC to connect to the NetWorker server.
5. Click **Configuration**, then click **Clients** in the left navigation pane.
6. Right-click the client that requires the client file index location update, and then select **Modify Client Properties**.
7. On the **Globals (2 of 2)** tab, in the **Index Path** attribute, specify the full path of the directory where the client file index now resides.
8. Click **OK**.

## Updating the index location for a client in NetWorker

**Procedure**

1. From the **Administration** window, click **Configuration**.
2. Click **Clients**.
3. Right-click the client with the client file index location to be changed, then select **Properties**. The **Properties** dialog box appears.
4. Click the **Globals (2 of 2)** tab.
5. In the **Index Path** attribute, enter the full path of the directory where the client file index now resides.
6. Click **Ok**.
7. (Optional) From a command prompt, run the `nsrck` or `nsrls` command and check the output for any errors.

For example, to run `nsrck` on client `jupiter`, type:

```
nsrck -L6 jupiter
```

Output similar to the following appears:

```
nsrck: checking index for 'jupiter'
nsrck: nsrindexesjupiter contains 54 records occupying 7 KB
nsrck: Completed checking 1 client(s)
```

**NOTICE**

Depending on the size of the client file index, running either `nsrck` or `nsrls` can take a considerable amount of time. Running the `nsrck -L6` command, as shown in the example, also checks the index for corruption.

If no problems are found, then all future client file index information is saved to the new location.

## Managing the size of the online indexes

Over time, the size of the online indexes on the NetWorker server can become prohibitively large. Reduce the size of these indexes by using the solutions suggested in these sections.

## Reduce the size of the client file index

You can reduce the size of the client file indexes on the NetWorker server by using one or more of these methods:

- Remove save sets that comprise the oldest backup cycle from the client file index. [Removing the oldest save set cycles on page 517](#) provides details.
- Delete volume-based entries from the client file index. [Deleting volume-based online index entries on page 518](#) provides details.
- Adjust the Browse Policy and Retention Policy attributes of clients backing up to the NetWorker server to shorten the period of time that entries remain in the client file indexes. This solution works only for client backups that occur after you change these policy attributes.
- Modify the browse policy associated with a particular save set by using the `nsrmm -w` command. Unless the associated save set contains a large number of files, this method may not be a practical method to reduce the index size. [Modifying the browse and retention policy on a save set on page 241](#) provides details.

If the size of the client file index for a client is still too large, consider moving the location of the index. [Moving a client file index on page 514](#) provides details.

## Reduce the size of the media database size

Use one or more of the following methods to reduce the size of media database on the NetWorker server.

- Remove volumes that contain recyclable save sets from the NetWorker inventory. [Removing volume-based entries from the online indexes on page 517](#) provides details. When you remove a volume from the media database, NetWorker removes the entries associated with that volume from the media database and the client file index for the client. If you select this option, you can use the `scanner` command to recover the data on the volume, if NetWorker has not relabeled the volume.

### NOTICE

You will gain very little disk space from removing a media database entry. Leaving index entries of a volume in the media database prevents the accidental labeling of another volume with the same name.

- 
- Recycle volumes that contain recyclable save sets. [Changing a volume's mode on page 209](#) provides details. When a volume mode changes to recyclable, the volume becomes eligible for reuse and NetWorker can performs the following operations:
    - Relabel the volume
    - Remove information about the save sets on the volume from the media database
    - Reinitialize the volume
 Once NetWorker relabels a volume, you cannot recover the contents.
 

To increase the number of currently recyclable save sets, modify the retention policy associated with the current media database by using the `nsrmm -e` command. [Modifying the browse and retention policy on a save set on page 241](#) provides details.
  - Compress the media database. [Compressing the media database on page 519](#) provides details.

## Removing the oldest save set cycles

Client file index entries for a full save set cycle include the last full backup and any dependent incremental or level saves. When you remove the oldest cycle, you free up disk space.

### Procedure

1. From the **Administration** window, click **Media**.
2. Click **Indexes**.
3. Right-click the appropriate client, then select **Show Save Sets**.
4. Select the save set with the oldest cycle to remove, then click **Remove Oldest Cycle**.
5. When prompted, click **Yes** to confirm the removal.

### Results

After the Remove Oldest Cycle operation has finished, NetWorker updates the statistics in the Index Save Sets dialog box to reflect the current state of the client file index.

## Removing volume-based entries from the online indexes

The main purpose of removing volume-based entries from the online indexes is to eliminate damaged or unusable volumes from the NetWorker server. You can also use this feature to reduce the size of the online indexes by purging index entries associated with specific volumes.

### Removing client file index entries

Use the `nsrmm` command to remove information about save set from the client file index. This changes the status of browsable save sets to recoverable.

### Procedure

1. At the command prompt, type:

```
nsrmm -d -P -S ssid
where ssid is the save set ID for the save set.
```

2. Use `mminfo` to determine the save set ID. At the command prompt, type:

### Results

```
mminfo -v -c client_name
```

The *EMC NetWorker Command Reference Guide* or the UNIX man pages provide information about the `nsrmm` and `mminfo` commands.

When NetWorker marks a save set as recoverable, you cannot browse to recover these files. Use the save set recover procedure to recover data from a recoverable save set. [Recovering the data on page 352](#) provides details.

### Removing client file index and media database entries

You can remove both the client file index and media database entries for a volume. This action removes all traces of the volume from the NetWorker server. Remove a volume from the media database only if the volume has been physically damaged and is unusable. However, if you remove the database entries for a volume, the volume is undamaged, and NetWorker has not relabeled the volume, you can use the `scanner` command to recover the data. [Recovering expired save sets on page 369](#) provides details.

Typically, do not remove both the client file index and media database entries at the same time unless the volume is damaged or destroyed.

#### NOTICE

The presence of a clone of a particular volume prevents the deletion of the volume entry in the media database. This is because the NetWorker server accesses the cloned volume rather than the original volume as needed. NetWorker does not purge the entry of the volume in the media database. Because of this functionality, removing volume entries from the media database is not a particularly effective way to reduce index size.

## Deleting volume-based online index entries

You can use NMC or the `nsrmm` command to delete volumes from the media database and client file indexes. The NetWorker server first cross-checks the indexes before it purges a volume. As a result, the volume might still appear in the **Volumes** window in NMC for a brief period of time.

### Procedure

1. From the **Administration** window, click **Media**.
2. Click **Volumes**.
3. Right-click the volume with the entry to delete from the online indexes, then select **Delete**.
4. Select one of these options to determine how volume entries will be removed:
  - **File and Media Index Entries.** [Removing client file index entries on page 517](#) provides details about this option.
  - **File Index Entries Only.** [Removing client file index and media database entries on page 517](#) provides details about this option.
5. Click **OK**.

### Deleting volumes from a command prompt

Use the `nsrmm` command to remove volume information from the media database and client file indexes.

To remove both client file index and media database entries for a volume, type the following command:

```
nsrmm -d -S ssid
```

To remove information about the volume from the client file index only, type the following command:

```
nsrmm -d -P volume_name
```

### Deleting volumes in NMC

Use NMC to remove volumes from the client file index or from both the media database and client file index.

### Procedure

1. From the **Administration** window, click **Media**.
2. Click **Volumes**.
3. Right-click the volume with the entry to delete from the online indexes, then select **Delete**.
4. Select one of these options to determine how volume entries will be removed:

- **File and Media Index Entries** to remove the volume information from the media database and client file indexes.
- **File Index Entries Only** to remove the volume information from the client file indexes only.

## Compressing the media database

You can free up more space on the server by compressing the media database.

### Procedure

1. Delete the appropriate file:
  - On Windows:  
`NetWorker_install_dir\mm\.cmprssd`
  - On UNIX:  
`/nsr/mm/.cmprssd`
2. Type the following command at the command prompt:  
`nsrim`

## Managing Client Push

The software distribution feature, Client Push distributes software and performs software updates to one or more NetWorker hosts from the NetWorker server.

The *EMC NetWorker Installation Guide* and the `nsrpush` man page describes how to use Client Push to update NetWorker products.

## Changing the location of the software repository

Use the `nsradmin` command to change the location of the software repository.

### Procedure

1. Log in to the NetWorker server as root on UNIX or administrator on Windows.
2. Connect to the `nsrcpd` database:
  - UNIX: `nsradmin -d /nsr/res/cpdb`
  - Windows: `nsradmin -d "NetWorker_install_path\nsr\res\cpdb"`
3. Set the current query type to *NSR Client Push Master*:

```
nsradmin> . type: NSR Client Push Master
Current query set
```

4. Review the current attribute settings:

```
nsradmin> print
          type: NSR Client Push Master;
          name: Client Push Master;
actual repository location: /nsr/repository;
default repository location: /nsr/repository;
exclude clients: ;
```

5. Update the *actual repository location* value:

```
nsradmin> update actual repository location: /new_repository
          actual repository location: /new_repository;
Update? y
updated resource id 0.2.15.116.0.0.0.43.78.222.34.14.10.5.172.45(7)
```

6. Confirm the value of the *actual repository location* attribute:

```
nsradmin> print
              type: NSR Client Push Master;
              name: Client Push Master;
              actual repository location: /new repository;
              default repository location: /nsr/repository;
              exclude clients: ;
```

7. Quit nsradmin.
8. End the nsrpd process on the NetWorker server.

## Removing software package information from the software repository

After you add new packages to the repository, you can remove old package information from the command line or from a GUI.

### Removing information from the repository by using the Software Administration Wizard

Use the Software Administration Wizard to remove information about software packages in the repository, from a GUI.

#### Procedure

1. Use NMC to connect to the NetWorker server.
2. On the **Configuration** menu, select **Software Administration Wizard...**
3. On the **Welcome to the Software Administration Wizard** window, click **Next**.
4. On the **Select Operation** window, accept the default **Add or remove products from my software repository**, then click **Next**.
5. On the **Software Repository Operations** window, select **Remove software products from the repository**, then click **Next**.
6. On the **Select Products to Remove** window, select the products you want to remove, then click **Next**.
7. If the remove operation completes successfully, then click **Ok** when the pop up window appears. If the remove operation fails, review the **nsrpd.raw** file located in the **/nsr/logs** (UNIX) or **NetWorker\_install\_path\nsr\logs** (Windows) directory for further details.

### Removing information from the repository by using the nsrpush command

Use nsrpush to remove information about software packages in the repository, from the command line.

Perform these steps from a command prompt on the NetWorker server as the administrator on Windows and the root account on UNIX.

#### Procedure

1. Display a list of products that are in the software repository:

For example:

```
nsrpush -l
Products in the repository
=====
NetWorker 8.1
win_x64
Storage Node
Server
```

```

License Manager
Language Packs
English Language Pack
French Language Pack
Japanese Language Pack
Korean Language Pack
Chinese Language Pack
Client
Management Console

```

## 2. Remove the packages:

```
nsrpush -r -p Product -v Version -P platform
```

For example, to remove the NetWorker 8.1 win\_x64 package:

```
nsrpush -r -p NetWorker -v 8.1 -P win_64
Remove from repository status: succeeded
```

If the remove operation fails, then review the nsrpd.raw file located in /nsr/logs on UNIX or NetWorker\_install\_path\nsr\logs on Windows for further details.

## Transferring files and folders by using nsrpush

You can use nsrpush to transfer files and folders from a central location to the /nsr directory on a UNIX host or the NetWorker\_install\_dir\nsr directory on a Windows host.

### Requirements for file and folder transfers

Before you transfer files and folders, ensure that the target host is in the Client Push inventory and there is sufficient free disk space in the tmp folder on the target host. Client push uses the c:\windows\temp folder on Windows and /tmp on UNIX.

When the operating system of the target host differs from the NetWorker server, for example, when the NetWorker server is on Windows and the target host is a UNIX, you must configure a proxy host to store the cross platform files and folders.

Before you select a proxy host, ensure that the host meets the following requirements:

- Is the same platform as the cross platform packages.  
For example, if the NetWorker server is a Linux host, use a Windows proxy host to transfer files to Windows x86, Windows x64, and Windows ia64 hosts.
- Has the NetWorker 7.6 or later client software installed.
- Is a client of the NetWorker server.

When you choose a directory on the proxy host to store the source files, ensure that the directory:

- Resides on a local file system.
- Uses a path that does not contain spaces or special characters.

## Transferring files and folders

You can transfer files and folders from a central location to all NetWorker hosts in a datazone or selected hosts. You can specify hosts in the nsrpush command or by using an input file.

From a command prompt on the NetWorker server, use nsrpush to the transfer files and folders.

## Performing cross platform file and folder transfers

To transfer files from the NetWorker server to NetWorker hosts on a cross platform operating system, the syntax of the `nsrpush` command is as follows:

```
nsrpush -Tx -c proxy_host -C proxy_source_path -U|-W -all|-If
input_file|hostname...
```

where:

- *proxy\_host* is the hostname of the host that contains the source files and folders.
- *proxy\_source\_path* is the folder on the Proxy host that contains the source files and folders.
- `-U` specifies a UNIX cross platform host and `-W` specifies a Windows cross platform. Use the appropriate option for the target host.
- `-all` transfers the source files and folders to all inventoried NetWorker hosts that are not in the exclude list.
- `-If input_file` transfers the source files and folder to all inventoried NetWorker hosts that are listed, one per line, in the input file. When specifying *input\_file*, include the name of the file and the path to the file on the NetWorker server.
- *hostname* is the name of the target host. Separate multiple hostnames with spaces.

Example: Transferring files from a proxy host

A NetWorker data zone uses a NetWorker 8.1 server on Windows and has two NetWorker UNIX clients, `pwd.emc.com` and `lad.emc.com` that require new DD Boost libraries in the `/nsr/bin` directory. The directory `/usr/ddlib/bin` on UNIX host `mnd.emc.com` contains the files.

To transfer the files, type: `nsrpush -Tx -c mnd.emc.com -C /usr/ddlib -U
pwd.emc.com lad.emc.com`

## Performing same platform file and folder transfers

To transfer files from the NetWorker server to same platform NetWorker hosts, the syntax of the `nsrpush` command is as follows:

```
nsrpush -Tx -m source_path -all|-If input_file|hostname...
```

where:

- *source\_path* specifies the path on the NetWorker server that contains the source files.
- `-all` transfers the source files and folders to all inventoried NetWorker hosts that are not in the exclude list.
- `-If input_file` transfers the source files and folder to all inventoried NetWorker hosts that are listed, one per line, in the input file. When specifying *input\_file*, include the name of the file and the path to the file on the NetWorker server.
- *hostname* is the name of the target host. Separate multiple hostnames with spaces.

Example: Transferring files from the NetWorker server

A NetWorker data zone uses a NetWorker 8.1 server on Windows and has two Windows clients, `dmd.emc.com` and `jad.emc.com` that require new DD Boost libraries. The directory `c:\ddlib` on the NetWorker server contains the files.

To transfer the files, type: `nsrpush -Tx -m c:\ddlib dmd.emc.com jad.emc.com`

## Troubleshooting file and folder transfers

This section describes how to troubleshoot file and folder transfer issues.

### Transfer media path doesn't exist: pathname

This error message appears when the source\_path or proxy\_source\_path specified in the nsrpush command does not exist on source or proxy host. To resolve this issue, ensure that you specify a valid path.

## Monitoring changes to the NetWorker and NMC Server resources

NetWorker provides two ways to monitor changes made in to the NetWorker and NMC server resources:

- Monitor RAP (resource allocation protocol) attribute in the NetWorker Server resource. This feature tracks both before and after information related to additions, deletions, or modifications to NetWorker server resources and their attributes.
- Security Audit Log feature. This feature provides the NetWorker server and the NMC Console server with the ability to log specific security audit events related to their operations.

The *EMC NetWorker Security Configuration Guide* describes how to use and configure the Monitor RAP attribute and the Security Audit Log feature.

## Disabling or enabling the Monitor RAP Attribute

The Monitor RAP attribute is enabled by default, to change the setting, perform the following steps in the Console window.

### Procedure

1. From the Administration window, select **View > Diagnostic Mode**.
2. Right-click the NetWorker server name in the left pane and select **Properties**.
3. In the **Setup** tab of the NetWorker Server Properties dialog box, select the **Monitor RAP Enabled** or the **Disabled** attribute as required.
4. Click **OK**.

## Log file size management

NetWorker stores messages generated by the NetWorker daemons or the Console server daemons in raw files. To manage the size of raw log files, modify attributes stored in the NSRLA database.

The *EMC NetWorker Security Configuration Guide* describes how to view, render, and manage raw log files.

## Internationalization

NetWorker releases 7.4 and later have been internationalized. As a result, the NetWorker software now supports language packs, which you can install as part of the NetWorker installation, or you can install the language packs separately after you have installed the NetWorker software. The *EMC NetWorker Installation Guide* provides more information.

Internationalization support in the NetWorker software depends on internationalization support of the underlying operating system. If you plan to use non-English data in the

NetWorker software, ensure that you install and configure the appropriate support for that language on the operating system.

The following sections describe a number of issues and limitations that relate to the use of NetWorker software in a multi-language environment.

## Log file viewer

To view NetWorker log files, use the `nsr_render_log` program. [Viewing log files on page 677](#) provide more information.

## Display issues

There are number of issues and limitations associated with displaying characters in various locales.

### Character display at the command line

From the command line, characters supported by the current locale display correctly. Characters that the current locale of the user do not support will not appear correctly. For Microsoft Windows systems, if the user and system locales do not match, characters supported in the user locale but not the system locale may not appear correctly.

### Character display in graphical user interfaces

How character display from within the different NetWorker GUIs vary and depend on the platform on which you run the GUI.

- On Microsoft Windows:
  - All Unicode encoded data will display correctly.
  - When you view UNIX path and filenames, path and filenames that you create with a character set that the current locale or UTF-8 supports, will display correctly. Paths that you create with another character set may not display correctly. Because Microsoft Windows does not have native support for many of the character sets used on UNIX (for example, euc-jp, euc-cn and euc-tw), if a non-ASCII character is encoded by using these character sets, characters will not display correctly on Microsoft Windows.
- On Unix:
  - Characters that the current locale does not support may not display correctly.
- On OS-X:
  - Differences in Unicode support, non-ASCII paths, and filenames on OS-X machines can result in characters not displaying correctly when you browse the file system from a non-Mac platform.

## Maximum path and save set length

For the NetWorker software, the maximum supported length for a pathname is twelve kilobytes, and the maximum length for a save set name is 1024 bytes. The number of characters allowed by each of these limits will vary depending on the locale.

All operating systems have an internal limit for path and filenames. The limit varies depending on the operating system and file system being used. Typically, the pathname component size is 256.

For Unix, only the path component length is checked against the limit. As a result, it is possible to create a path and filename that is greater than the limit supported by the operating system, but an attempt to access this path will result in a failure.

## Locale-specific configuration issues on UNIX/Linux

This section describes certain configuration issues related to Client and Archive Request resources for clients that run in UNIX/Linux environments.

### Configuring the Save Set attribute for Client and Archive Request resources

For clients that use non-ASCII locales on Unix platforms, or for clients on Microsoft Windows that you configure from a UNIX host that uses non-ASCII locales, special considerations apply when you type a path or filename in the Save Set attribute for Client or Archive Request resources.

You must enter the path or filename in the locale that was used when you created the path or file. If use a different locale when you enter a path or filename, subsequent backups will fail with the following error message:

```
No such file or directory
```

To configure a Client resource in this situation, either:

- Use the *All* keyword for the Save Set attribute.
- Log into a client host by using the correct locale, and then configure the client from this machine.

### Client resources with multiple locales on UNIX/Linux

To back up a UNIX or Linux machine that contains path or filenames with multiple locales, you must create a separate Client resource for each locale.

For example, to configure a multi-locale UNIX machine with data in both Japanese and French, you must create two different Client resources, one defining the save sets for the Japanese data, another defining the save sets for the French data.

[Creating multiple client resources for the same host on page 531](#) has information about creating multiple clients.

### Locale settings with NDMP

For NDMP backups, ensure that the locale setting is consistent in your environment.

Review the following requirements:

- Ensure that all UNIX locale settings on the filer (including UTF-8) are the same.
- Use an NMC client on a UNIX client set that has the exact same locale setting as the filer.

You can perform backup and recovery operations on any locale, but if you try to browse on host whose locale differs from the original locale, the filenames appear as random characters.

## Server communication issues within Microsoft Windows

This sections addresses various client/server communication issues that occur when running NetWorker software in a Microsoft Windows environment.

## Name resolution

If the network consists of only Microsoft Windows computers, you may find WINS or LMHOSTS is adequate for using NetWorker software. However, when using the software with clients running on other platforms, such as UNIX, you must use a local host file or DNS name resolution.

You must add the NetWorker server name to either the local hosts file (located in %SystemRoot%\system32\drivers\etc) or the Domain Name Server that contains the names of all servers on your network.

## Backup Operators group

The Microsoft Windows Backup Operators local group provides its members the privileges necessary to back up and recover data from a Windows computer.

Users who request backups must be in the Backup Operators or Administrators group of the domain into which they are logged. The Backup Operators group is assigned on a computer-by-computer basis, rather than globally by the domain. If you are having trouble performing tasks on one NetWorker server but not another, check Backup Operators group on the problematic computer to ensure that you are properly assigned.

## Dynamic Host Configuration Protocol

A NetWorker server requires a static (fixed) hostname address. Typically, addresses for Dynamic Host Configuration Protocol (DHCP) clients change because they use dynamic addressing. If the address changes, the authorization code for that NetWorker server becomes invalid. If the NetWorker server is a DHCP client, a static TCP/IP address for the server must be preserved. NetWorker clients can still use dynamic addressing.

## Backup and Recover Server service

In Microsoft Windows operating systems, the NetWorker Backup and Recover Server service is normally started by the Windows System account. This allows backup and recovery services to run even if no one is logged onto that computer.

# CHAPTER 19

## NetWorker Client Management

This chapter contains the following topics:

- [NetWorker client overview](#)..... 528
- [Client configuration](#)..... 528
- [Create a lockbox to store and retrieve pass phrases securely](#)..... 531
- [NetWorker authentication](#)..... 531
- [Creating multiple client resources for the same host](#)..... 531
- [Scheduled backups of non-ASCII files or directories](#)..... 532
- [Controlling access to a NetWorker client](#)..... 533
- [Client priority](#)..... 533
- [Dedicated client/server interface for backup and recovery operations](#)..... 534

## NetWorker client overview

A NetWorker client is a physical computer that you install the NetWorker client software on, and a NetWorker server resource that specifies a set of files and directories that a scheduled backup should include. A single NetWorker client computer can have several Client resources specified that can back up to the same or even different NetWorker servers.

[Defining a client and save set combination on page 532](#) provides more information about a client computer with multiple NetWorker Client resources.

EMC provides the NetWorker client software for a variety of operating system platforms. Any NetWorker server can backup a NetWorker client, regardless of the platform the client resides on. For example, you can back up a NetWorker client on a Microsoft Windows computer to a NetWorker server on a Solaris computer.

## Client configuration

Before a NetWorker server can backup a client, install the appropriate NetWorker client software on the client machine. The *EMC NetWorker Installation Guide* provides more information.

### Creating a client

You create a NetWorker client resource on the NetWorker server during the process of creating a scheduled backup. [Scheduled backup creation on page 61](#) describes how to create a client.

### Editing a client

After you create a NetWorker client resource on the NetWorker sever, you can modify the client resource attributes.

#### Procedure

1. From the **Administration** window, click **Configuration**.
2. Click **Clients**.
3. Right-click a client, then select **Properties**. The **Properties** dialog box appears, with the **General** tab displayed.
4. Edit the attributes of the client, then click **OK**.

### Copying a client

Use this procedure to create a copy of the Client resource.

#### Procedure

1. From the **Administration** window, click **Configuration**.
2. Click **Clients**.
3. Right-click a client, then select **Copy**. The **Create Client** dialog box appears. By default, the new client retains the information from the client that was copied, except the **Name** attribute, which is blank.
4. Enter the name for the new client and edit other attributes as appropriate, then click **OK**.

## Changing a client name

The only way to change the name of a client is to re-create the client. Use this procedure to delete the client resource and create a new client resource with the new name.

### Procedure

1. From the **Administration** window, click **Configuration**.
2. Click **Clients**.
3. Right-click the client resource to be renamed, then select **Properties**.
4. Click the **Globals (1 of 2)** tab.
5. Record the **Client ID** attribute listed for the client, then click **Cancel** to close the **Properties** dialog box.
6. Delete the original client resource from the **Administration** window.
7. Stop all of the NetWorker services on the NetWorker server.
8. On the NetWorker server that backs up this client, rename the directory that contains the client file index for this client from `old_client_name.domain.com` to `new_client_name.domain.com`. The default location for the client file index is:
  - For UNIX/Linux:  
`/nsr/index/client_name.domain.com`
  - For Microsoft Windows:  
`NetWorker_install_path\index\client_name.domain.com`
9. Restart the NetWorker services on the NetWorker server.
10. Create a new client resource. Ensure that you enter the client ID that you recorded in step 5.

## Deleting a client

When you delete a client, the NetWorker server can no longer back up or recover files from the client computer. The backup history for the client remains in the client file index and media database until the entries are removed. Perform the following steps to delete a client resource.

### Procedure

1. From the **Administration** window, click **Configuration**.
2. Click **Clients**.
3. Right-click the client to be deleted, then select **Delete**.
4. When prompted, click **Yes** to confirm the deletion.

---

### Note

After you delete the client resource, you can still access and recover previously backed-up data for the client directly from the volume that contains the data by using the scanner command.

---

## Recreating a deleted client

To recreate a deleted client, create a new client resource. Ensure that the value that you specify in the Name attribute on the General tab of the Create Client dialog box is the name value of the original client resource.

The NetWorker server recalls the client ID for this name and inserts it into the Client ID attribute on the Globals (1 of 2) tab of the Create Client dialog box.

## Hostname changes

NetWorker considers each unique client name as a separate client. NetWorker assigns each unique client name in the datazone a unique identifier called a client ID. NetWorker stores the client ID for each client in the media database.

When you change the name of a NetWorker client in the datazone and delete the NetWorker client resources, ensure that you create the new client resource with the new hostname and the clientID that NetWorker assigned to the original NetWorker client.

[Recreating a deleted client on page 530](#) provides more information.

If you create the new client resource but do not use the clientID of the original NetWorker host:

- The NetWorker server will consider the new hostname to be a new NetWorker host.
- The NetWorker server will assign the new hostname a new clientID.
- To recover data, you must perform a directed recover from the original hostname to the new hostname.
- You cannot perform a browsable recovery, only a save set recovery.

To resolve this issue, use the `nsrclientfix` command to analyze the media database and identify client ID inconsistencies. You can also use the `nsrclientfix` command to merge information about multiple clients in the media database and resource database into one client resource with the original client ID. KB article 000185727 on the [EMC Support website](#) describes how to use the `nsrclientfix` command to identify and correct client ID inconsistencies.

## Editing a client NSRLA database

The NetWorker Client database, `nsexec` contains a NetWorker resource, called the NSRLA resource. The NSRLA resource contains information about the client and attributes that you can modify. Use the character-based `nsradmin` program to modify the MSRLA resource.

### Procedure

1. Log in as root or as Windows Administrator on the NetWorker client.
2. Type this at the command prompt:

```
nsradmin -p nsexec
```

The `nsradmin` prompt appears.

3. To determine the current settings for attributes in the NSRLA resource, perform the following two steps:
  - a. To determine the current settings for any hidden attributes (such as the Disable Directed Recover attribute), type the following at the `nsradmin` prompt:
 

```
option Hidden
```

b. To display attributes, type the following:

```
print type:NSRLA
```

4. To change the value of attributes in the **NSRLA** resource, type this line at the **nsadmin** prompt:

```
update attribute:value;
```

For example, to update the Disable Directed Recover attribute, type: **update disable directed recover:Yes**

#### Note

[Directed recoveries on page 348](#) provides information about permissions and requirements for directed recoveries.

5. Type **Yes** when prompted to confirm the change.

#### Results

##### NOTICE

When you modify an attribute with the **nsadmin** program, you must specify the attribute name and value correctly. If you do not specify the attribute name and value correctly, the **nsadmin** program does not update the attribute and **nsadmin** does not provide an error message.

The *EMC NetWorker Security Configuration Guide* provides more information about the **nsexec** database and how to modify attributes in the **nsexec** database.

## Create a lockbox to store and retrieve pass phrases securely

The NetWorker server provides NetWorker modules, and certain NetWorker features, such as AES encryption, with the ability to securely store and retrieve passwords over a network by using a NetWorker lockbox.

The *EMC NetWorker Security Configuration Guide* describes how to use the lockbox feature and how to configure NetWorker to use AES encryption.

## NetWorker authentication

NetWorker supports two types of authentication between hosts, **nsrauth** and **oldauth**. The *EMC NetWorker Security Configuration Guide* provides more information.

This product should only be used where network-layer authentication prevents rogue hosts from connecting or accessing network traffic.

## Creating multiple client resources for the same host

The NetWorker server uses the host name to identify each client. To provide optimal flexibility, you can create multiple client resources for the same host name, when the configuration meets one of the following requirements:

- Each Save set attribute for each client contains a unique value.
- Each client resource is in a different backup group.
- Each client resource uses a different backup schedule.

- Each client resource uses a different browse and/or retention policy.

For example, when you look at the list of configured NetWorker clients, you might see several instances of a client named mars, but each instance would backup a unique collection of save sets, use different schedules or policies or would have different group membership.

You can define multiple clients for the same host or file system when you need to back up specialized files, such as databases. For example, configure one client resource to back up filesystems at a different time than another client resource instance configured to back up the database files. You can use the Comment attribute in the Client resource to help distinguish between multiple Client resources with the same name.

## Redefining a large file system backup into multiple client and save set instances

When a client system has a large amount of backup data, configure multiple clients with different save sets to back up the data at different times. Redefining a large file system into multiple client and save set instances that start at different times, enables you to load balance a full backup of the entire filesystem. If different backup start times do not reduce the load adequately, you can associate each client resource with a different backup schedule that performs a full backup on a different day of the week.

[Schedules on page 256](#) provide more information on schedules.

## Defining a client and save set combination

The same save set can appear in the Save set attribute of the Client resource for multiple client instances. This characteristic enables you to associate the same save set with more than one group or schedule for backup.

If the default value All appears in the Save Set attribute, then NetWorker will backup all of the local data for the host, according to the group and schedule associated with the client. To define a different client and save set combination, perform the following steps:

### Procedure

1. Create a new or edit an existing NetWorker client.
2. On the **General** tab in the **Save Set** attribute, delete the default value **All**.
3. Perform one of the following steps:
  - To configure the client to back up a specific file system, type the file system pathname in the **Save Set** attribute.
  - To define multiple save sets on a client, type each save set (partition, file system, or file) on a separate line in the **Save Set** attribute.

## Scheduled backups of non-ASCII files or directories

If you did not create the client resource with the Client Backup Configuration Wizard and the Save set attribute contains non-ASCII characters, you must modify the Save Operation attribute in the Client resource.

- UNIX/Linux clients:  
**I18N:mode=nativepath**
- Windows clients:  
**I18N:mode=utf8path**

## Controlling access to a NetWorker client

NetWorker uses the contents of the `/nsr/res/servers` (UNIX), or the `NetWorker_install_path\res\servers` (Windows) file on each NetWorker client to control who has client-tasking rights. Client-tasking rights provide a host with the right to request a program execution on another client). The following table provides a list of tasks that require an update to the servers file.

**Table 95** When to modify the servers file

| Operations              | Update required on the NetWorker client's servers file                                                                                                               |
|-------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Archive request         | Add the long and shortname of the NetWorker server.                                                                                                                  |
| Scheduled backup        | Add the long and shortname of the NetWorker server.<br>For a clustered NetWorker server, add the long and shortname of the virtual NetWorker and all physical nodes. |
| Remote Directed Restore | Add the long and shortname of the administering client to the server file on the destination client.                                                                 |
| NDMP DSA backups        | Add the long and shortname of the NetWorker client that initiates the backup.                                                                                        |

The *EMC NetWorker Security Configuration Guide* provides more information about client-tasking rights and how to modify the servers file.

## Client priority

The Priority attribute in the Client resource specifies the order in which the NetWorker server contacts clients for backup. The attribute can contain a value between 1 and 1,000. The lower the value, the higher the priority.

During a backup operation, the NetWorker server contacts the client with the lowest value for the Priority attribute first. If the client resources do not contain a value in the Priority attribute, the backup order is random.

While the Priority attribute specifies the order of client contact, many variables affect the order in which clients complete their backups. For example:

- The backup operation on a client does not begin until the worklists for each of the save sets on the client are complete.
- The amount of work can vary greatly from one client to the next.
- If a client stops responding and times out, then the backup operation puts the client backup at the end of the backup order list.

To increase the number of times the backup operation will retry a backup for each client in a group before the backup attempt is considered unsuccessful, change the value in the Client Retries attribute in the Group resource. [Creating groups for backup clients on page 63](#) provides more information.

---

### Note

The only way to guarantee that the backup of ClientA occurs before ClientB is to assign ClientA to a scheduled backup group that starts earlier than the group that contains ClientB.

## Dedicated client/server interface for backup and recovery operations

You can configure NetWorker clients to use a unique network interface on the NetWorker server and storage node for backup and recovery operations. [Using multihomed systems on page 666](#) provides more information.

# CHAPTER 20

## Block Based Backup and Recovery

This chapter contains the following topics:

|                                                                                |     |
|--------------------------------------------------------------------------------|-----|
| • <a href="#">Overview</a> .....                                               | 536 |
| • <a href="#">Preparing for block based backups</a> .....                      | 538 |
| • <a href="#">Performing block based backups</a> .....                         | 541 |
| • <a href="#">Verifying block based backups</a> .....                          | 543 |
| • <a href="#">Cloning block based backups</a> .....                            | 544 |
| • <a href="#">Performing block based recoveries</a> .....                      | 544 |
| • <a href="#">Performing block based clone recoveries</a> .....                | 547 |
| • <a href="#">Troubleshooting block based backup and recovery issues</a> ..... | 549 |

## Overview

The NetWorker block based backups are high-performance backups that support NTFS and ReFS file systems.

During the block based backups, the backup application scans a volume or a disk in a file system, and backs up all the blocks that are in use in the file system. Block based backups use the following technologies:

- The Volume Shadow Copy Service (VSS) snapshot capability to create consistent copies of the source volume for backups.

- The Virtual Hard Disk (VHDx), which is sparse, to back up data to the target device.

The block based backups support only the following Client Direct enabled devices as target devices:

- Advanced File Type Devices (AFTDs)
- Data Domain devices

The block based incremental backups use the Change Block Tracking (CBT) driver to identify the changed blocks, and back up only the changed blocks.

**NOTICE**

You must install the latest recommended service packs and VSS patches.

The block based full and incremental backups are fast backups with reduced backup times because the backup process backs up only the occupied disk blocks and changed disk blocks respectively. Block based backups can coexist with traditional backups.

The block based backups provide instant access to the backups. The block based backups enable you to mount the backups by using the same file systems that you used to back up the data. For example, if the data that you backed up is NTFS, you can mount the block based backup by using NTFS.

The block based backups provide the following capabilities:

- Mounting of a backup as a file system
- Maximum of 38 incremental backups after a full backup
- Mounting of an incremental backup
- Sparse backup support
- Backups to disk-like devices
- Backups to Data Domain
- Backups of operating system-deduped file systems as source volumes
- Virtual full backups to Data Domain
- Synthetic full backups to AFTD
- Incremental synthetic full backups to AFTD
- Backups of volumes up to 63 TB each
- Recoveries from Data Domain without using CIFS share
- Recovery of multiple save sets in a single operation
- Image recoveries without mounting the backup image

The following table lists the backup scenarios and the recovery scenarios that the block based backups support.

**Table 96** Supported backup and recovery scenarios

| Backup scenarios                                                                                                                                                                                                                                                                                                                                                                                                                                  | Recovery scenarios                                                                                                                                                                                                                                                                                   |
|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <ul style="list-style-type: none"> <li>• AFTD backups</li> <li>• Backups to Data Domain by using DD Boost</li> <li>• Full backups</li> <li>• Virtual full backups</li> <li>• Synthetic full backups</li> <li>• Incremental backups</li> <li>• Incremental synthetic full backups</li> <li>• Full backups and incremental backups intermixed with built-in provisions to anchor the incremental backups with an appropriate backup type</li> </ul> | <ul style="list-style-type: none"> <li>• File level recovery by mounting the backup image on a target host</li> <li>• Image/destructive recovery at the block level</li> <li>• Image/destructive recovery from clones</li> <li>• Windows Bare Metal Recovery (BMR) by using a WinPE image</li> </ul> |

## Supported operating systems and configurations

The block based backups support the backup and recovery of the following operating systems and configurations:

- Operating systems on x64:
  - Windows client 8.1
  - Windows client 8
  - Windows Server 2012 R2
  - Windows Server 2012
  - Windows Server 2008 R2
- Operating systems on x86:
  - Windows client 8.1
  - Windows client 8
- Client Direct target devices
- Concurrent backups of multiple volumes
- Windows Server 2012 and Windows Server 2012 R2 deduplicated volumes without rehydrating the deduplicated data
- Windows Server core installation role
- Unified Extensible Firmware Interface (UEFI) based systems
- GUID Partition Table (GPT) and Master Boot Record (MBR) volumes
- Data Domain systems in a Fibre Channel environment
- Full backup of Windows Server 2012 Cluster Shared Volumes on File Servers and Windows Clusters
- Full and incremental backups of New Technology File System (NTFS) and Resilient File System (ReFS)

## Limitations

The block based backups do not support the following capabilities and configurations:

- FAT file system
- Backup levels 1 through 9
- Cloning of incremental backups
- Granular save sets at either the folder level or the file level, for example, D:\data
- Checkpoint restart
- Standard NetWorker directives
- The scanner command with the -i option for rebuilding indexes for block based backups
- Staging and the nsrclone command with the -m option for migrating block based backup save sets to other volumes
- Image recovery to a system volume
- Recoveries of ReFS volumes on Windows Server 2008 R2 and Windows 8 (x86 and x64)
- Recoveries of dedupe volumes on Windows Server 2008 R2 and Windows 8 (x86 and x64)

## Preparing for block based backups

You must create a backup device and configure block based backups before you perform block based backups and recoveries. Also, you can create a CIFS share for block based recoveries.

### Creating a backup device

You can create the following types of devices that depend on the backup requirements.

- AFTD
- Data Domain CIFS
- DD Boost

#### Creating an AFTD or a Data Domain CIFS device

Use one of the following methods to create an AFTD:

- [Creating an AFTD by using the Device Wizard on page 158](#)—describes how to create an AFTD by using the NMC wizard.
- [Creating an AFTD by using the Properties window \(Windows\) on page 163](#)—describes how to create an AFTD by using the New Device Properties dialog box.

**NOTICE**

If you want to make a local AFTD Client Direct enabled, specify the Uniform Naming Convention (UNC) path in the **Device access information** field of the **Create device properties** dialog box.

## Creating a DD Boost device

### Procedure

1. In NMC, click **Devices**.
2. In the left panel, right-click **Devices** and select **New Device Wizard**.
3. On the **Select the Device** page, select **Data Domain** and click **Next**.
4. On the **Data Domain Preconfiguration Checklist** page, click **Next**.
5. On the **Specify the Data Domain Configuration Options** page:
  - a. Under **Data Domain System Name**:
    - Select **Create a New Data Domain System**.
    - In the text box, type the IP address of the Data Domain system.
  - b. In the **Data Domain DDBlOst Username** field, type the username of the Data Domain user.
  - c. In the **Data Domain DDBlOst Password** field, type the password of the Data Domain user.
  - d. Specify the required values in the other fields.
  - e. Click **Next**.
6. On the **Select the Folder to Use as Devices** page:
  - a. Click **New Folder** to create a folder for the device.
  - b. Select the newly created folder.
  - c. Specify the required values in the other fields.
  - d. Click **Next**.
7. On the **Configure Pool Information** page:
  - a. Under **Pool Type**, select one of the following pool types:
    - Backup
    - Backup Clone
  - b. Under **Pool**, perform one of the following tasks to select the pool:
    - Select **Create and use a new pool**, and type the pool number in the text box.
    - Select **Use an existing pool**, and select the pool from the drop-down list box.
  - c. Specify the required values in the other fields.
  - d. Click **Next**.
8. On the **Select Storage Nodes and Fibre Channel Options** page:
  - a. Select the storage node.
  - b. Specify the required values in the other fields.
  - c. Click **Next**.
9. On the **Select SNMP Monitoring Options** page, specify the required field values, and click **Next**.
10. On the **Review the Device Configuration Settings** page, review the configuration settings, and click **Configure**.

11.On the **Device Configuration Results** page, click **Finish**.

## Configuring block based backups

### Procedure

1. Enable the block based backup feature when you use one of the following methods to configure the client:
  - NetWorker Client Configuration wizard
  - Client Properties window
  - The nsadmin program
2. Select the following fields to enable the block based backup feature:
  - Client direct (selected by default)
  - Block based backup

## Creating a CIFS share for block based recoveries-Optional

You must enable a CIFS share to access save sets on the device to recover data from either a Data Domain device or an AFTD.

### Creating a CIFS share on a Data Domain device

#### Procedure

1. Open Data Domain Enterprise Manager.
2. In the left panel, under **DD Network**, select the Data Domain device.
3. Click **Data Management**.
4. Click **CIFS**.
5. Click **Shares**.
6. Click **Create**.
7. In the **Create Share** dialog box:
  - a. In the **Share Name** field, type the NetWorker server short name.
  - b. In the **Directory Path** field, type the full pathname of the share folder, which is available on the Data Domain device, in the following format:  
*/data/coll/NetWorker\_server\_short\_name*
  - c. In the **Clients** field, add either the IP addresses or the hostnames of the clients from which you want to access the CIFS share.
  - d. Click **OK**.
8. Access the CIFS share from the clients.
9. If you want to add more clients after creating a share, click **Modify**.

### Creating an AFTD CIFS share on Windows

The access credentials are the same as the administrator's credentials on the host.

#### Procedure

1. Right-click the folder that you want to share, and select **Share with > Specific people...**

2. In the **File Sharing** dialog box, select or add the people with whom who want to share the folder, and click **Share**.

## Performing block based backups

The procedure for performing a block based backup is the same as the procedure for performing a NetWorker backup.

[Backing Up Data on page 59](#) provides more information about how to back up data by using NetWorker.

You can perform a block based backup as any of the following types of backup:

- Scheduled backups
- Incremental backups
- Virtual full backups
- Synthetic full and incremental synthetic full backups
- Manual backups or client-initiated backups
- Save set backups
- Exclude list backups
- Windows deduplication volume backups
- CSV backups
- Windows BMR backups

### Scheduled backups

The NetWorker `savegrp` program supports the block based backups for all scheduled backups.

The scheduled backup process is transparent to you and does not require any additional actions or considerations.

### Incremental backups

The NetWorker `savegrp` program initiates a scheduled backup as either a full backup or an incremental backup.

You must perform the incremental backup of a volume only to the same device to which either you or another user performed the full backup of the volume.

An incremental backup shifts to a full backup when any of the following conditions occur:

- You restart the client host for any reason when the backup is either in progress or scheduled.
- The preceding incremental backup failed.
- You already performed 38 incremental backups.

---

#### Note

After you perform a full backup, you can perform a maximum of 38 incremental backups.

- 
- You add a volume for the backup of the All save set.
  - You change the size of the volume.

The incremental backup process is transparent to you and does not require any additional actions or considerations.

## Virtual full backups

The virtual full backups apply only to the Data Domain devices. When you perform an incremental backup to a Data Domain device, you perform the backup as a virtual full backup. However, the type of the backup that you have performed is displayed as full. A virtual full backup backs up only the changed blocks from its previous full backup while referencing the unchanged blocks to the corresponding blocks of the previous full backup.

---

### Note

Selecting any backup level apart from full results in performing a virtual full backup. The block based backup enables you to perform 38 virtual full backups only, after which the subsequent backup shifts to the full backup.

---

## Synthetic full and incremental synthetic full backups

The synthetic full and incremental synthetic full backups apply only to AFTDs. A synthetic full backup consolidates data from all the existing full and incremental backups. An incremental synthetic full backup first performs an incremental backup from the immediate previous backup and then performs a synthetic full backup.

---

### Note

When you perform an incremental synthetic full backup to a non-Windows remote storage node, you must create a client configuration for the storage node.

---

## Manual backups or client-initiated backups

Use the save command with the -z option to perform a client-initiated block based backup from the command line.

Ensure that you meet the following requirements for a client-initiated backup:

- The device must be Client Direct enabled.  
You can provide a pool of Client Direct enabled devices by using the save command with the -b option.
- The client-initiated block based backup supports the full level save sets that you define only at the volume level.

## Save set backups

You can use a block based backup to back up the following save sets:

- All—This save set includes VSS volumes, critical volumes, and non critical volumes.
- DISASTER\_RECOVERY—This save set includes VSS volumes and critical volumes.
- Volumes—Specify any type of volume drive letters as save sets. For example: D:\
- Volume mount points—Specify volume mount points as save sets. For example: D:\mount\_point\_name (for a single mount point)  
D:\mount\_point\_name1\mount\_point\_name2\mount\_point\_name3 (for nested mount points)

## Exclude list backups

The exclude list backups exclude the files that the operating system specifies as unwanted files in the `HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\BackupRestore\FilesNotToBackup` Registry key. Also, the backup excludes unsupported writers and application files such as SQL, Exchange, and so on. However, the backup does not exclude the files that are present in the system volume information.

## Windows deduplication volume backups

The block based backups occur at the block level. The file system layout does not affect the backup. The backup virtual hard disk is deduplication in nature. The block based backups merge the blocks out of the deduplication volumes. In case the volume changes from deduplication to non-deduplication, the block based backup detects these events and forces the next backup to be a full backup.

## CSV backups

You can simultaneously see Cluster Shared Volumes (CSVs) across all nodes. The block based backups support only full backups of CSVs, even in the case of a failover. If you try to perform an incremental backup, the backup shifts to a full backup with a warning message.

For non-CSV volumes, if a failover happens after an incremental backup, the backup shifts to a full backup.

## Windows BMR backups

The procedure for performing a block based backup as a Windows BMR backup is the same as the procedure for performing a NetWorker Windows BMR backup. However, you must select the Block based backup option when you configure the client by using the NetWorker Client Configuration wizard, the Client Properties window, or the `nsradmin` program.

[Windows Bare Metal Recovery on page 611](#) provides more information about BMR backups.

## Verifying block based backups

### Procedure

- Run the following command:

```
mminfo -S -q save_set_ID
```

- From the output, see whether the following information is present:

\*BlockBasedBackup: Yes;

For virtual full backups and synthetic full backups, see whether the following additional information is present respectively:

- \*BlockBased Virtual Full: Yes;
- \*Synthetic full: Yes;

## Cloning block based backups

The procedure for cloning a block based backup is the same as the procedure for cloning a NetWorker backup.

You can configure the NetWorker clone operations according to the environment and storage requirements. The block based backups support cloning of the full backups only.

[Cloning on page 319](#) provides more information about cloning the NetWorker backups.

Run the following command to clone the block based backup save sets:

```
nsrclone-b target_pool_name -S save_set_ID/clone_ID
```

## Performing block based recoveries

You can perform block based recoveries by using either the NMC or the NetWorker CLI.

### Preparing for block based recoveries

You must be familiar with the recovery operations, workflows, and interfaces that associate with the block based recovery. Use either NMC or the NetWorker command-line interface (CLI) to perform a block based recovery.

You typically complete the following tasks to perform a recovery by using NMC:

1. Selecting the save set.
2. Performing either file level recovery or image/destructive recovery.

If you want to perform a recovery by using the CLI, you must run the `recover.exe` command with the save set ID. Unlike a traditional backup, the block based backup does not maintain any indexes in the NetWorker client file index database.

The recovery process mounts all the save sets on a device that supports the Client Direct functionality.

If you want to recover data from either an AFTD or a Data Domain device by using the CIFS share, you must enable the CIFS share to access save sets on the device.

[Preparing for block based backups on page 538](#) provides information about how to create the CIFS share and devices.

### Using NMC to perform block based recoveries

#### Procedure

1. Open NMC.
2. Click **Recover**.
3. From the menu bar, select **Recover > Recover > New Recover**.
4. On the **Select the Client to Recover** page:
  - a. Under **Source client**, in the **Name** field, type the name of the client on which the backed-up data exists.
  - b. Under **Destination client**, specify the client to which you want to recover the backed-up data.
  - c. For the type of backup that you want to recover, select **Block Based Backup**.

- d. Click **Next**.
5. On the **Select the Data to Recover** page:
  - a. Select one of the following types of recovery that you want to perform:
    - File level recovery
    - Image level recovery
  - b. Select the timestamp of the backup that you want to recover.
  - c. Perform one of the following tasks that depend on the type of the recovery that you have selected:
    - For a file level recovery:
      - In the left panel, select the save sets that you want to recover.
      - In the right panel, select the relevant files that you want to recover.
    - For an image level recovery, in the left panel, select the save set that you want to recover.
  - d. Click **Next**.
6. On the **Select the Recovery Options** page, perform one of the following tasks that depend on the type of the recovery that you have selected:
  - For a file level recovery, select the **File path for Recovery** and **Duplicate File Options** and click **Next**.
  - For an image level recovery, select the **File path for Recovery** and click **Next**.
7. On the **Obtain the Volume Information** page, click **Next**.
8. On the **Perform the Recovery** page:
  - a. Under **Identity**, in the **Recover name** field, type a name for the recovery.
  - b. Select one of the following recovery start times:
    - **Start recovery now**—Immediately starts the recovery.
    - **Schedule recovery to start at**—Schedules the recovery according to your choice.
  - c. If you want to stop the recovery at a certain time, in the **Specify a hard stop time** field, type the time.
  - d. Select the **Recover Resource persistence** option according to your choice.
  - e. Click **Run Recovery**.

The recovery log appears when the recovery progresses.

After the recovery succeeds, a successful completion message appears at the bottom of the recovery log.

To export the log file, click **Export Log File**.
9. On the **Check the Recovery Results** page, click **Finish**.

## Using the CLI to perform block based recoveries

Use the `recover.exe` command to perform a block based recovery. The command applies only to local clients. However, you cannot use the command to perform a remote or redirected recovery.

## Performing a file level recovery

### NOTICE

If you want to avoid using the Windows version of the recover.exe command on Windows operating systems, perform one of the following tasks:

- Include `NetWorker_install_path\bin\recover.exe` at the command prompt.
- Ensure that the `$PATH` environment variable lists `NetWorker_install_path\bin` before `%SystemRoot%\System32`.

### Procedure

1. Run the following command to mount the backup and start the command prompt at the mount point:

```
recover.exe -S save_set_ID
```

Use the Windows copy option and paste option to recover the backup.

After you perform the recovery, close the command prompt to exit the process.

2. Run the following command to mount the backup and copy specific files from the input file to the destination:

```
recover.exe -S save_set_ID -I input_file -d destination
```

## Performing image and destructive recoveries

Ensure that you meet the following requirements to perform a recovery:

- The size of the target volume is either the same or bigger than the size of the source volume.
- The cluster size of the source volume is the same or bigger than the cluster size of the target volume.

Run the following command to mount the source volume, unmount the target volume, and copy the used blocks on the source volume to the target volume:

```
recover.exe -S save_set_ID -r target_volume
```

### Note

Ensure that the target volume is not a system volume.

## Command-line options for recover.exe

The following table describes the key options that you can use with the `recover.exe` command to perform a block based recovery.

**Table 97** Key options for the block based recover.exe command

| Option                                    | Description                                                                                                                                                                |
|-------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <code>-r [volume GUID/mount point]</code> | Specifies the supported destinations for save set recovery: <ul style="list-style-type: none"> <li>• Volume name</li> <li>• Raw pathname</li> <li>• Volume GUID</li> </ul> |

**Table 97** Key options for the block based recover.exe command (continued)

| Option                    | Description                                                                                                                            |
|---------------------------|----------------------------------------------------------------------------------------------------------------------------------------|
|                           | <ul style="list-style-type: none"> <li>Existing mount point</li> </ul>                                                                 |
| -k [mount/unmount]        | Specifies to mount or unmount a save set.                                                                                              |
| -S [save set ID/clone ID] | Specifies the save set ID or the clone ID that you want to recover.                                                                    |
| -l [input file]           | Specifies a file that contains a list of files that you want to recover. This is useful to perform the disaster and remote recoveries. |

## Performing Windows BMR

The procedure to recover a block based backup through a Windows BMR is the same as the procedure to perform a NetWorker Windows BMR. However, you must select an appropriate block based backup on the Select System Recovery page of the wizard when you perform the block based recovery.

## Performing block based clone recoveries

You can recover cloned data from the Client Direct enabled devices and the Client Direct disabled devices.

### Recovering data from Client Direct enabled devices

Client Direct enabled devices include AFTD, DD Boost, and Data Domain CIFS devices.

Use one of the following methods to recover the data:

- NMC  
Perform the steps that the [Using NMC to perform block based recoveries on page 544](#) section describes.
- NetWorker CLI  
Run one of the following commands:
  - `recover.exe -S save_set_ID/clone_ID`  
for file level recoveries
  - `recover.exe -S save_set_ID/clone_ID -r target_volume`  
for image recoveries

### Recovering data from Client Direct disabled devices

Client Direct disabled devices typically include tape devices.

The file level recovery process requires a Client Direct enabled device. The recovery process first temporarily stages the data to a Client Direct enabled device that you have selected and then recovers the data from the device. The retention period of the staged data on the Client Direct enabled device is three days. You can delete the data before the retention period lapses.

The image recovery process by using the GUI is the same as the process to perform a file level recovery. However, you can perform image recoveries directly from the tape devices without mounting the backup images by using the CLI.

Use either the NMC or the recover.exe command to perform recoveries.

## Using the NMC to perform the clone recovery

### Procedure

1. Open the NMC.
2. Click **Recover**.
3. From the menu bar, select **Recover > Recover > New Recover**.
4. On the **Select the Client to Recover** page:
  - a. Under **Source client**, in the **Name** field, type the name of the client on which the cloned data exists.
  - b. Under **Destination client**, specify the client to which you want to recover the cloned data.
  - c. For the type of backup that you want to recover, select **Block Based Backup (cloned to tape)**.
  - d. Click **Next**.
5. On the **Select a Block-Based Backup Clone** page:
  - a. Under **Found in**, specify the period during which you performed the clone and click **Query**.  
The cloned save set groups appear in the **Block-Based backups** field.
  - b. Select the save set group.
  - c. Under **Select the Save Sets**, select either **All save sets** or **Subsets of save sets** and appropriate save sets that belong to the selected save set group.
  - d. Under **Pool**, select the pool that has the Client Direct enabled device to which you want to copy the cloned data.
  - e. Click **Next**.  
The **Copying the Backup to Disk** page appears.
  - f. After the cloning succeeds, click **Next**.
6. On the **Select the Data to Recover** page:
  - a. Select one of the following types of recovery that you want to perform:
    - File level recovery
    - Image level recovery
  - b. Select the timestamp of the backup that you want to recover.
  - c. Perform one of the following tasks that depend on the type of the recovery you have selected:
    - For a file level recovery, select the save set to recover from the left panes and select the files to recover from the right panes.
    - For an image level recovery, select the save set that you want to recover from the left pane.
  - d. Click **Next**.
7. On the **Select the Recovery Options** page, perform one of the following tasks that depend on the type of the recovery you have selected:

- For a file level recovery, select the **File path for Recovery** and **Duplicate File Options** and click **Next**.
  - For an image level recovery, select the **File path for Recovery** and click **Next**.
8. On the **Obtain the Volume Information** page, click **Next**.
9. On the **Perform the Recovery** page:
- a. Under **Identity**, in the **Recover name** field, type a name for the recovery.
  - b. Select one of the following recovery start times:
    - **Start recovery now**—Immediately starts recovery.
    - **Schedule recovery to start at**—Schedules the recovery according to your choice.
  - c. If you want to stop the recovery at a certain time, in the **Specify a hard stop time** field, type the time.
  - d. Select the **Recover Resource persistence** option according to your choice.
  - e. Click **Run Recovery**.
- The recovery log appears when the recovery progresses.
- After the recovery succeeds, a successful completion message appears at the bottom of the recovery log.
- To export the log file, click **Export Log File**.
10. On the **Check the Recovery Results** page, click **Finish**.

### Using the CLI to perform the clone recovery

Run one of the following commands to recover the data from the Client Direct disabled devices:

- `recover -S save_set_ID/clone_ID -l pool_name`  
for file level recoveries  
The pool that you select must have a Client Direct enabled device. The pool must also be a backup clone pool.
- `recover -S save_set_ID/clone_ID -r target_volume`  
for image recoveries

## Troubleshooting block based backup and recovery issues

This section lists the common issues with the block based backups and recoveries and provides workarounds for these issues.

**Table 98** Troubleshooting block based backup and recovery issues

| Error message or Issue                                                                                                                                                     | Resolution                                                         |
|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------|
| Block based backups are only supported with Client Direct.                                                                                                                 | In the Client Properties dialog box, select <b>Client Direct</b> . |
| VSS OTHER: ERROR: VSS failed to process snapshot: The shadow copy provider had an unexpected error while trying to process the specified operation. (VSS error 0x8004230f) | Ensure that there is no recover session running on the client.     |

**Table 98** Troubleshooting block based backup and recovery issues (continued)

| Error message or Issue                                                                                                                         | Resolution                                                                                                                                                                            |
|------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 90108:save: Unable to save the SYSTEM STATE<br>save sets: cannot create the snapshot.                                                          |                                                                                                                                                                                       |
| No save sets clone to clone device.                                                                                                            | Block based backups clone only full backup save sets. Block based backups do not clone incremental backup save sets.                                                                  |
| Unable to construct the recover list from input file.                                                                                          | Perform an image recovery if applicable. Otherwise, select all the files except the system files such as, System Volume Information and Recycle Bin to perform a file level recovery. |
| Failed to recover save set with error: To perform the recovery of a block based backup save set, the device must be enabled for Client Direct. | In the Client Properties dialog box, select <b>Client Direct</b> .                                                                                                                    |

# CHAPTER 21

## NetWorker support for NDMP

This chapter contains the following topics:

- [Overview of NDMP](#) ..... 552
- [Components in a NetWorker NDMP environment](#) ..... 552
- [Configurations in a NetWorker NDMP environment](#) ..... 552
- [Pre-configuration requirements for NDMP data operations](#) ..... 557
- [Configuring Devices for NDMP operations](#) ..... 560
- [Creating resources to support NDMP clients](#) ..... 568
- [Creating and configuring the NDMP client resource](#) ..... 569
- [Performing NDMP backups](#) ..... 578
- [Troubleshooting NDMP configuration and backup failures](#) ..... 580
- [Cloning NDMP save sets](#) ..... 584
- [Reporting NDMP Data](#) ..... 585
- [Performing NDMP recoveries](#) ..... 586
- [Troubleshooting NDMP recover](#) ..... 595

## Overview of NDMP

The network data management protocol (NDMP) is a TCP/IP-based protocol that specifies how network components talk to each other for the purpose of moving data across the network for backup and recovery.

The NDMP protocol addresses the problems associated with backing up data in heterogeneous environments when you use different operating system vendors, backup developers, and Network Attached Storage (NAS) devices.

NDMP enables disparate vendors to use a common NDMP protocol for the backup architecture. With the NetWorker NDMP interface, you can connect to hosts that have an active NDMP Service or an NDMP data module installed. You do not install the NetWorker software on the NDMP host. NDMP allows a NAS device to back up data to other NDMP-controlled tape or disk devices that are on the network. NDMP passes control of the data and the file metadata to and from the NetWorker software.

The NetWorker server by default attempts to establish communications with a NAS filer by using NDMP version 4. If the NAS does not support or use NDMP v4, communications are autonegotiated to use the highest version that the NAS filer supports. NetWorker supports NDMP v3 and later however, there are some NetWorker features that require a specific version of NDMP on the NAS.

The *EMC NetWorker Hardware Compatibility Guide* on the EMC Online Support web site provides a list of NAS filers that the NetWorker software supports.

## Components in a NetWorker NDMP environment

Three main components support NDMP data operations with the NetWorker software.

- NDMP Data Server—The system that contains the NDMP data. The NDMP Data Server is also known as the datamover, the NDMP client, or the NAS filer. The NAS transfers the data to the primary storage devices through a data connection. You configure the NAS as a client of the NetWorker server; however, you do not install the NetWorker client software on the NAS.
- NDMP Tape Server—The host with the backup device to which NetWorker writes the NDMP data.
- Data Management Agent(DMA)—The NetWorker server is the DMA.  
The DMA:
  - Initiates the NDMP backup.
  - Monitors the NDMP backup and recover operations.
  - Maintains the media database and the client file index entries for NDMP backups.
  - Maintains the resource database information for the NAS and NDMP Tape Server.

## Configurations in a NetWorker NDMP environment

You can use three methods to configure the NDMP Data Server and the NDMP Tape Server to perform backups and recoveries. You can customize the NetWorker environment to support NDMP data operations in each scenario:

- [NDMP local backup on page 553](#)—The NDMP Data Server and the NDMP Tape Server reside on the same physical host.

- [NDMP backups to non-NDMP devices \(NDMP-DSA\) on page 554](#)—An NDMP Data Server Agent (NDMP-DSA) sends the NDMP data from the NDMP Data Server to the non-NDMP devices.
- [Three-party backup with NDMP devices on page 556](#)—The NDMP Data Server and the NDMP Tape Server reside on different physical hosts. The NAS passes NDMP metadata to the NetWorker server. The NetWorker server sends the data to an NDMP tape device attached to another NDMP Server.

The following table summarizes the differences between the NDMP Tape Server and NDMP-DSA.

**Table 99** Distinctions between NDMP Tape Server and NDMP-DSA

| NDMP Tape Server                            | NDMP-DSA                                                          |
|---------------------------------------------|-------------------------------------------------------------------|
| Supports only the NDMP type of tape device. | Supports any type of device that the NetWorker software supports. |
| Does not support backup to disk.            | Supports backup to disk.                                          |
| Does not support multiplexing.              | Supports multiplexing.                                            |

## NDMP local backup

In an NDMP local backup (Direct-NDMP), the NDMP Data Server (NAS) sends data to a locally attached tape device or library. The `nsrndmp_save` program runs on the NetWorker server, and only the metadata and the NDMP control information traverse the network between the NetWorker server and the NDMP host.

### Advantages:

The NDMP data does not traverse the network, this prevents network congestion.

### Disadvantages:

- The `nsrndmp_save` program queries the NDMP Tape Server at consistent intervals to determine the status of a backup. These queries have an impact on backup performance.
- The NetWorker software does not multiplex NDMP save sets and writes NDMP data serially to the local device. As a result, backups are faster, but recoveries are slower.
- NDMP local backups are not suitable when there are many large file systems to back up on a NAS filer.
- You cannot archive NDMP save sets.

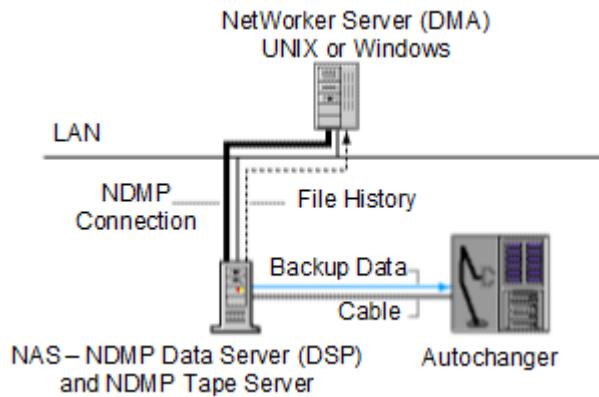
The NetWorker server, or data management application (DMA), performs these tasks:

- Initiates the backup or the recovery request through the NDMP connection.
- Receives the file history information from the data server.

During a backup, the NAS filer is the NDMP Tape Server and the NDMP Data Server. The NAS filer performs these tasks:

- Receives the backup requests.
- Reads the backup data on the NAS disks.
- Produces a data stream for the backup.
- Writes the data stream to the tape or file device.

The following figure illustrates a local backup configuration.

**Figure 34** NDMP local backup configuration

## NDMP backups to non-NDMP devices (NDMP-DSA)

In this scenario, the NetWorker software writes NDMP data to non-NDMP devices, including tape, disk, optical, and Data Domain devices. Use NDMP-DSA backups when there are many small file systems to backup, and network throughput is not a concern. An NDMP data backup to disk is faster than an NDMP backup to tape. Directing NDMP staged and cloned data to a non-NDMP device is faster than sending the data to an NDMP device.

The NetWorker software uses the NDMP Data Server Agent (DSA) and the `nsrndmp_save` command to send NDMP data to a non-NDMP device. The process associated with DSA is `nsrdsa_save`.

The benefits of using NDMP-DSA include the ability to:

- Write NDMP data to devices that also contain non-NDMP data.
- Multiplex NDMP save sets to improve backup speeds. Recovery speeds are slower
- Stage save sets from the disk to tape.
- Archive NDMP save sets.

You can back up NDMP data to a non-NDMP device in one of two ways:

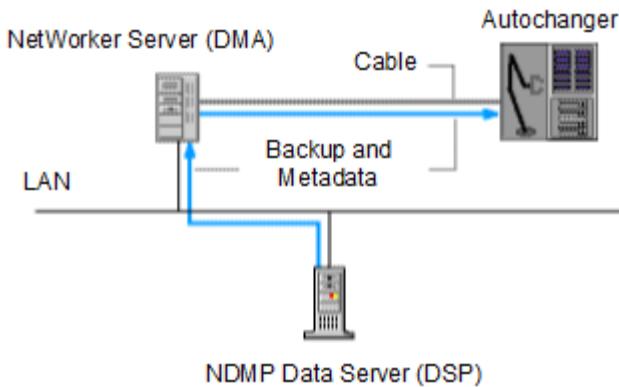
- NDMP data sent to non-NDMP devices that are local to the NetWorker server.
- NDMP data sent to non-NDMP devices that reside on a NetWorker storage node.

### NDMP data sent to non-NDMP devices that are local to the NetWorker server

When you send NDMP data to non-NDMP devices that are local to the NetWorker server:

- The backup data traverses the network between the NetWorker server and the NDMP Data Server.
- The metadata, the NDMP control information, and the FH remain local to the NetWorker server and do not traverse the network.

The following figure illustrates a NetWorker storage device directly attached to the NetWorker server. The NetWorker server initiates an NDMP-DSA backup. The `nsrmmmd` process on the NetWorker server processes the data and metadata. The `nsrndmp_2fh` and `nsrddmpix` processes on the NetWorker server process the file history (FH) data and then pass the FH data to the `nsrindexd` process.

**Figure 35** Backup initiated from a NetWorker server with an attached storage device

### NDMP data sent to non-NDMP devices that reside on a NetWorker storage node

You can configure NDMP backups to write data to a NetWorker storage node in one of three ways.

#### Immediate save

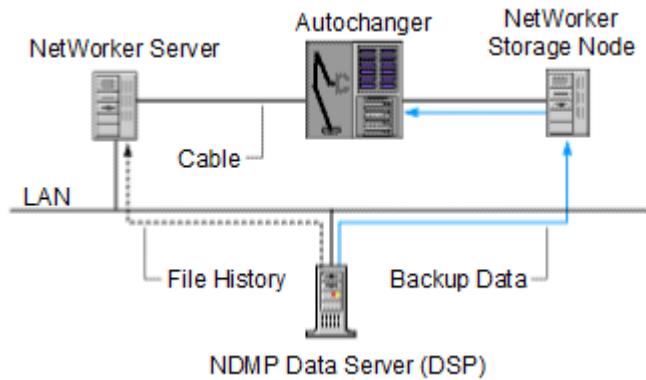
When you configure an NDMP backup with immediate save, the following actions occur.

1. The `nsrdsa_save` backup command runs on the NetWorker storage node.
2. The NetWorker software uses TCP/IP and shared memory to communicate between the `nsrdsa_save` and `nsrmmd` processes.
3. The NetWorker server processes the backup data and sends the data to the non-NDMP device directly through the `nsrmmd` process on the storage node.

When the NetWorker software uses immediate save to send the NDMP data, the following actions occur.

- The `nsrindexd` process on the NetWorker server processes the file history.
- After the data backup completes and the sessions with the NDMP Data Server and the NetWorker server close, the NetWorker software commits the FH to the client file index associated with the NDMP client.

The following figure illustrates a NetWorker configuration that uses immediate save.

**Figure 36** NDMP backup that uses immediate save

## Non-immediate save

By default, NDMP backups to a non-NDMP device uses non-immediate save.

When you configure an NDMP backup to use non-immediate save, the following actions occur:

1. The `nsrdsa_save` backup command runs on the NetWorker server.
2. The `nsrdsa_save` process uses TCP/IP to read the data in a local buffer.
3. The `nsrdsa_save` process transmits the data to the `nsrmmd` process on the storage node.
4. The `nsrmmd` process writes the data to the storage device.

This approach is inefficient and has slow performance for the following reasons:

- Backup data traverses the network between the NetWorker server, the NDMP host, and the NetWorker storage node.
- Metadata and the NDMP control information traverse the network between the NetWorker server and the storage node.
- FH traverses the network between the NetWorker server and the NDMP Data Server.

## Client Direct file access

Use Client Direct file access technology only when you perform an NDMP backup to a disk such as an advanced file type device (AFTD). Client Direct writes the data directly to disk, and bypasses the `nsrmmd` process on the storage node. The storage node only plays a role in loading the volume. This is a highly efficient, high-performance approach.

## Three-party backup with NDMP devices

A three-party backup, or three-way backup, sends NDMP data to an NDMP Tape Server, but the NDMP Data Server and the NDMP Tape Server are not the same physical host.

There are two types of three-party backups:

- The NetWorker software sends the NDMP data to non-NDMP devices. [NDMP backups to non-NDMP devices \(NDMP-DSA\) on page 554](#) provides more information.
- The NetWorker software sends NDMP data to NDMP devices. In this scenario, the data flows from the NDMP Data Server to the NDMP Tape Server, and then to a library locally attached to the NDMP Tape Server. In this configuration, you cannot archive the NDMP save sets.

In addition to using a NetWorker server or storage node as the NDMP Tape Server, you can use these third party NDMP Tape Servers:

- NetWorker SnapImage Module 2.5 or later.
- A DinoStor TapeServer. This hardware connects one or more libraries to the network and allows you to back up any NDMP host to one location instead of requiring a local backup device for each server.

The following figure demonstrates a three-party configuration, which enables backup and recovery to a NDMP device attached to another NDMP server.

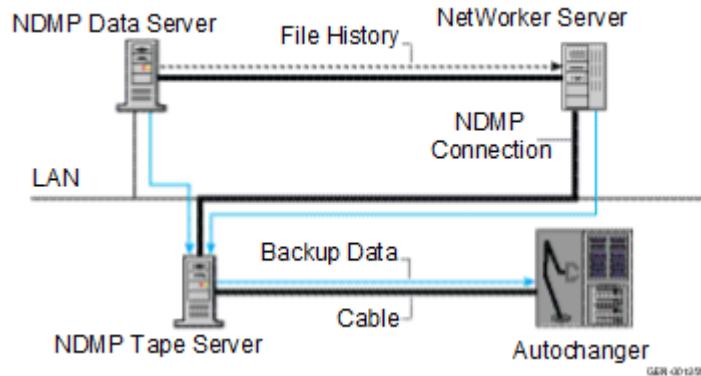
In this example:

- One server is the data server.
- The second server is the tape server.

- The third party is the NetWorker server (DMA).

This configuration is similar to the flow of data between a NetWorker client and a NetWorker server or storage node, except that it is not necessary to install the NetWorker software on either of the NDMP hosts. Data flows from the NDMP Data Server over the network to the NDMP Tape Server and then to tape. The NDMP Data Server sends the metadata to the NetWorker server.

**Figure 37** Three-party NDMP backup to NDMP devices



## Pre-configuration requirements for NDMP data operations

This section provides the requirements to review before you configure the NetWorker software for NDMP data operations.

### Note

The *EMC NetWorker Security Configuration Guide* describes how to determine port requirements for NDMP backups and recoveries when a firewall exists in the NetWorker datazone.

## NDMP feature requirements

Before you implement the Checkpoint restart, SMTape, iSCSI, vbb, and DAR/DDAR features in NetWorker, review the information in the following table.

**Table 100** NDMP features

| Feature            | Information                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |
|--------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Checkpoint restart | <ul style="list-style-type: none"> <li>Supports NetApp and Isilon filers only.</li> <li>Requires NDMP v4 restartable backup extension.</li> <li>Enabling checkpoint restart support for the NDMP client results in slower backups because NetWorker writes the checkpoint files at defined intervals. The more frequently NetWorker writes checkpoint files, the slower the backup.</li> <li>You cannot use NetWorker 7.6.x and earlier to restore a checkpoint restarted NDMP backup. <a href="#">Checkpoint restart backups on page 92</a> provides more information about checkpoint restarts.</li> </ul> |

**Table 100** NDMP features (continued)

| Feature                     | Information                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |
|-----------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Snapmirror to tape (SMTape) | <p>Performs block-level backup of SnapMirror volumes on NetApp filers. Reduces the backup window when millions of files reside on the NetApp filer.</p> <p>Use the SMTape feature in instances where NDMP full backups become impractical.</p> <p><b>SMTape:</b></p> <ul style="list-style-type: none"> <li>• Copies large NetApp file systems to secondary storage instead of using the standard NDMP full or differential backups</li> <li>• Supports a 240 KB block size.</li> <li>• Allows mirroring of backups to disk and tape devices.</li> <li>• Supports full volume backups and recoveries only. You cannot use SMTape for file indexes or file restores.</li> <li>• Supports save set recoveries, only.</li> <li>• Does not support incremental and differential backup levels.</li> </ul> <p>The NAS generates a snapshot of the file system at the beginning of the SMTape operation. Use Environment variables to control the conditional call to retain or delete the snapshot. <a href="#">“Creating and configuring the NDMP client resource on page 569</a> describes how to configure an NDMP client by using SMTape.</p> |
| iSCSI                       | <p>NetWorker supports iSCSI LUNS on EMC Celerra and NetApp filers. EMC Celerra filers do not support NDMP based backups and recoveries of iSCSI LUNS.</p> <p>NetApp filers support NDMP based backups and recoveries of iSCSI LUNS but you cannot perform an index-based recovery. To perform a full save set recover to another volume, the destination volume must be at least two and a half times as large as the source volume.</p> <p>NetApp recommends using SnapMirror to safeguard iSCSI LUNS instead of backups.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |
| vbb                         | <p>vbb supports:</p> <ul style="list-style-type: none"> <li>• EMC DART version 5.5 and later.</li> <li>• Index-based recoveries of a Celerra or VNX block level to the same volume or another location.</li> </ul> <p>Use:</p> <ul style="list-style-type: none"> <li>• Checkpoint configuration utility to configure checkpoint file systems on the EMC Celerra or VNX before you perform a backup.</li> <li>• Full Destructive Restore (FDR) to perform a full save set recovery of a raw volume of equal or greater size than the backup.</li> </ul> <p>NetWorker performs a file-by-file recovery when you:</p> <ul style="list-style-type: none"> <li>• Recover data from a Celerra or VNX block-level backup. This recover requires disk space in the root directory of the target filesystem to store temporary recovery files.</li> <li>• Perform save set recoveries and NDMP Directory Restores to an existing file system.</li> </ul>                                                                                                                                                                                             |

**Table 100** NDMP features (continued)

| Feature      | Information                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                |
|--------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|              | <p>When you backup a volume that uses native Celerra deduplication, you cannot perform an index-based or NDMP Directory Restore of the backup. You can only perform an FDR restore from a level FULL save set.</p> <p><i>Configuring NDMP backups on Celerra and Using Celerra Data Deduplication on EMC Support Online</i> provides detailed information about how to prepare the filer before you perform FDR.</p>                                                                                                       |
| DAR and DDAR | <p>DAR and DDAR sends file information from the NAS filer to NetWorker. This allows a single file recovery or a directory recovery to position to the exact location of the data on the tape media. NetWorker does not read the file and record numbers sequentially to locate the data.</p> <p>You cannot use DDAR when you enable vbb.</p> <p>Supports EMC DART version 5.5 or later and NetApp with OnTap version 6.4 and later.</p> <p>Requires NDMP version 3 or later. Recoveries on earlier NDMP versions fail.</p> |

## Locale requirements with NDMP

When running NDMP backups, ensure that you use consistent locale settings in the environment.

- NetWorker supports the UTF-8 format with CIFS clients. NetWorker only supports NFS clients of a NetApp filer when the NFS clients can generate UTF-8 encoded data. If you set the *UTF8=Y* variable during an NDMP backup and the backup contains path names with non-ASCII characters, then index-based recoveries of the backup fail with an error message similar to the following:

```
"RESTORE: could not create path pathname"
```

- If you use *UTF8=Y* and perform a backup, then you must recover path names that contain non-ASCII characters by using either a save set recovery from the command line or an NDMP Directory restore.
- All UNIX locale settings on the NAS filer, including UTF-8 must be the same.
- Configure the NAS filer to use UTF-8 character sets. Contact the NAS vendor for configuration requirements.
- Use only UNIX Console clients that have the same locale setting as the NAS filer.
- You can perform backup and recovery operations on any locale. However, if you try to browse on a locale that is different from the original locale, then the file names appear as random characters.
- A single save set supports data that belongs to only one code set. If you have data in multiple code sets, you must create multiple save groups. [Creating resources to support NDMP clients on page 568](#) describes how to create groups for NDMP clients.
- A save set can contain filenames that belong to different languages if all characters in those languages belong to the same code set. For example ISO 8859-1 and ISO 8859-15 include most Western European languages, such as French, Spanish, and

Portuguese. NetWorker can back up filenames from these languages in a single save set.

## Memory and space requirements for NDMP FH updates

During an NDMP backup, the NDMP Data Server sends the FH metadata information to the NetWorker server. The NetWorker software does not verify or modify FH metadata received from the NAS. The NetWorker software uses the file history information to maintain appropriate indexes and media database entries for the NDMP client backups.

The `nsrndmp_2fh` and `nsrdmpix` binaries interact with the raw database, instead of virtual memory, to process the FH metadata. As a result, memory requirements for this process are minimal. The NetWorker server stores metadata updates in the `\nsr\tmp` directory and commits the metadata to the client file index after the NDMP client backup completes.

Use the following formula to determine the required physical space for the default `\nsr\tmp` directory:

$$2 * (144 + \text{average file name length}) * \text{number of entries in the file system}$$

For example:

For one million file entries with an average file name length of 128, use this formula to compute the required temporary swap space:

- $2 * (144 + 128) * 1,000,000 = 544 \text{ MB approximately}$

## Performance Considerations

Volume loading and positioning operations do not occur during a volume selection process because of an information exchange between the `nsrmmd` process and the `nsrndmp_save` or `nsrndmp_recover` command. To avoid the overhead associated with the exchange of information, back up the data to a storage node device.

On NetApp filers with Data OnTap 6.4 and later, NetWorker reads all metadata from tape before recovering the files. For large save sets with 20 million files or more, the recovery time for a file can exceed three hours. This also applies to backups because NetWorker records the metadata for the whole volume onto the tape during a single file backup.

## NDMP licensing requirements

NetWorker with NDMP requires an additional license, separate from the NetWorker base product according to a tiered or capacity-based licensing structure. The *EMC NetWorker Licensing Guide* provides more information.

## Configuring Devices for NDMP operations

Review this section for information about how to configure the NetWorker environment for NDMP data operations:

The *EMC NetWorker Hardware Compatibility Guide* on the EMC Online Support web site provides a list of NDMP devices that the NetWorker software supports.

## NDMP device limitations

Review these limitations before you configure NDMP devices.

- The NetWorker server resource attributes named, `nsrmmd` control timeout, does not apply to NDMP devices but it does apply to storage nodes devices.

- You cannot use the jbexercise utility with an NDMP autochanger.
- You cannot configure NDMP devices on a dedicated storage node.
- NDMP media device handle must be a non-rewind device handle.
- You cannot configure Advanced file type devices and file type devices as an NDMP device.
- You cannot configure an NDMP Autochanger when the NDMP protocol is before version 3. You must determine the NDMP device handles, then use the `jbconfig` command to configure the autochanger. [Determining NDMP device path names on page 561](#) provides more information.

## DinoStor-managed jukeboxes

The DinoStor software provides a web-based interface for administering and controlling the TapeServer settings.

Review this information before you use a DinoStor-managed jukebox with NetWorker:

- When you configure the DinoStor TapeServer, set the port number to 10000 on the NDMP page of the Configure tab.
- NetWorker supports:
  - SCSI tape devices.
  - GigE and 10/100 Base-T networks.
- You cannot use DDS because the DinoStor TapeServer is not fibre-equipped.

## Configuring NDMP on Isilon filer

Before you can backup NDMP data, you must configure OneFS NDMP.

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

## Determining NDMP device path names

To configure an NDMP standalone device or NDMP jukebox, you must first determine the path names of the media devices. If the NAS filer does not support the NDMP\_CONFIG interface or uses NDMP version 3, you must also determine the library device handle.

To determine the NDMP device path names and the library handle, use the `inquire` command or vendor-specific commands:

### Determining the NDMP device path names by using inquire

Use the `inquire` command to determine the path names and library handle.

### Procedure

1. From a command prompt on the NetWorker server, type:

```
inquire -N NAS_hostname -T
```

- When prompted, specify the NAS username and password.

**NOTICE**

Use the inquire command with caution. When you run inquire, the command sends the SCSI inquiry command to all devices detected on the SCSI bus. If you use the inquire during normal operations, then unforeseen errors can occur, resulting in possible data loss.

## Determining the NDMP path names with vendor-specific commands

Before you configure an NDMP autochanger you must determine the device path names of NDMP devices and the robotic arm. The following table provides vendor-specific information that you can use to determine the device path names.

**Table 101** Determining NDMP path names

| NAS                 | Vendor specific information to determine autochanger and device paths                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |
|---------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| EMC Celerra and VNX | <p>Use the Celerra or VNX Administrator program or manually query the scsidevs file. To manually query the scsidevs file, log in to the filer with the ndmp account and type:</p> <pre>server_devconfig data_mover_name=p -s -n</pre> <p>The host responds with a list of media device names, for example:</p> <pre>server_2 :<br/>Scsi device table<br/>name addr type info<br/>jbox1 c1t0l0 jbox ATL P1000 62200501.21<br/>tape2 c1t4l0 tape QUANTUM DLT7000 245Fq_<br/>tape3 c1t5l0 tape QUANTUM DLT7000 245Fq_</pre> <p>To help avoid tape drive issues, set the ntape parameter for every tape drive discovered on a particular Data Mover. For example, if a Data Mover has five tape drives configured on it, set the parameter to <i>NDMP ntape=5</i>. To modify the <i>NDMP ntape</i> parameter, edit the /nas/server/slot_#/param file, where slot_# correlates directly to the server number and reboot the filer. You cannot specify a value greater than 8 for ntape. Configuring NDMP on EMC Celerra on the EMC Online Support web site provides detailed information about configuring an EMC Celerra filer.</p> |
| Isilon              | <p>For an NDMP local backup only, configure Backup Accelerator: Use the isi fc list command to ensure that the state of each fibre channel ports is enabled.</p> <p>Use the isi tape rescan --reconcile command to scan for tape devices. --reconcile deletes the device entries for devices that a Backup Accelerator node no longer manages.</p> <p>Use the isi tape ls -v to display a list of current devices.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |
| DinoStor-managed    | <p>Access the DinoStor TapeServer interface.</p> <ol style="list-style-type: none"> <li>Click the <b>Configure</b> page.</li> <li>Click the SCSI tab.</li> <li>Make note of the device names and device handles.</li> </ol>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     |

**Table 101** Determining NDMP path names (continued)

| NAS                | Vendor specific information to determine autochanger and device paths                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             |
|--------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| MiraPoint          | <p>On the MiraPoint filer, type:<br/> <code>diag tape inquiry ** ** **</code></p> <p>The device pathname is in the format <code>/dev/nrstn</code>, where <i>n</i> starts at 0 and increases one number for each tape drive. This value is constant.</p> <p>When the filer uses NDMP v2, or does not support the NDMP_CONFIG interface, you must specify the autochanger handle, <code>/dev/ch0</code>, when running the <code>jbconfig</code> command.</p> <p>To determine the autochanger handle, type:<br/> <code>diag changer inquiry ** ** **</code></p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |
| NetApp             | <p>Log in to the appliance as root or as a Windows Administrator and type:<br/> <code>sysconfig -t</code></p> <p>The host responds with a list of media device names, for example:</p> <pre>Tape drive (DS_300B:3.126L10) Hewlett-Packard LTO-4 nrst01 - no rewind device, format is: LTO-2(ro)/3 2/400GB nrst0m - no rewind device, format is: LTO-2(ro)/3 4/800GB cmp nrst0h - no rewind device, format is: LTO-4 800GB nrst0a - no rewind device, format is: LTO-4 1600GB cmp</pre> <p>where:</p> <ul style="list-style-type: none"> <li>• <code>(DS_300B:3.126L10)</code> indicates the switch (DS_3--6), the port number (3) and the LUN number( 10). This information must match the output in the <code>sysconfig -v</code> command.</li> <li>• <code>nrst01</code> is the media device name.<br/> When the filer uses NDMP v2, or does not support the NDMP_CONFIG interface, to determine the autochanger handle, type:<br/> <code>sysconfig -m</code></li> </ul> <p>The host responds with the devices on the host, for example:</p> <pre>Medium changer (DS_300B:3.126L9) ADIC Scalar i2000 mc5 - medium changer device</pre> <p>where <code>mc5</code> is the autochanger handle.</p> |
| Procom<br>NetFORCE | <p>Log in as root and type: <code>status dm</code></p> <p>If the filer uses NDMP v2 or does not support the NDMP_CONFIG interface, you must determine the autochanger handle.</p> <p>On a Procom NetFORCE filer, the SCSI device name format is <code>isp1tSSL[L]</code>, where <code>isp1</code> is the autochanger handle. The Fibre Channel device format is <code>ffx1tSSL[L]</code>, where <code>ffx1</code> is the autochanger handle.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |

## Configuring NDMP devices

You can back up NDMP data to an NDMP or non-NDMP device in a standalone or library configuration. You can also back up NDMP data to ACSLS controlled silos.

## Configuring a standalone NDMP device

Use NMC to configure a standalone NDMP tape device for Direct NDMP backups.

### Procedure

1. In the **Administration** window, click **Devices**.
2. Right-click **Devices** in the navigation tree, and select **New**.
3. In the **Name** attribute, specify the NDMP device in the format:

```
rd=NAS_hostname:NAS_device_handle (NDMP)
```

where:

- **NAS\_hostname** is the hostname of the NAS that has the NDMP device attached.
- **NAS\_device\_handle** is the path of the device.

**NOTICE**

You must configure the NDMP device as a remote device and you must add **(NDMP)** after the pathname. Otherwise, you will receive a message similar to the following:

---

**NDMP device name shall be in rd=<snode>:<devname (NDMP)> format**

---

4. In the **Media Type** attribute, specify the appropriate device type.
5. Specify a valid NAS administrator account in the **Remote User** attribute.

**NOTICE**

For an EMC Celerra and VNX filers, specify the trusted account created for backup on each NDMP-Host Data Mover. Some EMC Celerra versions require that you use a trusted account named *ndmp*. Configuring NDMP on EMC Celerra on the EMC Online Support web site provides detailed information.

---

6. Specify the password for the NAS administrator account in the **Password** attribute.
7. Under the **Configuration** tab:
  - a. Select the **NDMP** checkbox. You can only set this attribute when creating the device. You cannot change the NDMP attribute after you create the device. To change the device configuration, you must delete and recreate the device.
  - b. Set the **Target Sessions** attribute to **1**. NDMP devices do not support multiplexing.
  - c. The **Dedicated Storage Node** attribute must remain at the default value: **No**.
8. Under the **Advanced** tab, the **CDI** attribute must remain at the default value: **Not used**.
9. Optionally, change the block size the NDMP device uses. By default, NDMP devices use a block size of 60 KB. If required, select a different block size in the **Device block size** field. When you configure the NDMP client, you must set the **NDMP\_AUTO\_BLOCK\_SIZE** environment variable in the **Application Information** attribute. [Table 104 on page 571](#) provides more information.
10. Click **OK**.

## Configuring an NDMP autochanger

You can use an NDMP autochanger to manage Direct NDMP or Three-party backups with NDMP devices. To configure an NDMP autochanger, use NMC or the `jbconfig` command.

### Configuring an NDMP autochanger with NMC

When you configure an NDMP autochanger in NMC, the NetWorker software first detects the NDMP devices and then configures the library.

#### Procedure

1. In the **NetWorker Administration** window, click **Devices**.
2. Right-click on the NetWorker Server and then select **Configure All Libraries**.
3. In the **Provide General Configuration Information** window, accept the default library type, **SCSI/NDMP**, and then click **Next**.
4. In the **Select Target Storage Nodes** window, click **Create a new Storage Node**.
5. In the **Storage Node Name** field, specify the hostname of the NAS. If a DinoStor TapeServer manages the autochanger, specify the DinoStor hostname.
6. Select **ndmp** in the **Device Scan Type** attribute.
7. In the **NDMP User Name** and **NDMP Password** fields, specify the NAS administrator account. If DinoStor TapeServer manages the autochanger, specify the DinoStor username and password.
8. Click **Start Configuration**.
9. Click **Finish**.

10. Monitor the **Log** window for the status of the device scan.

When you specify an incorrect username and password combination:

- The Log status window reports:

```
No configured libraries detected on storage node
storage_node_name
```

- The `daemon.raw` file on the NetWorker server reports:

```
NDMP Service Debug: The process id for NDMP service is
0xb6c0b7b0
42597:dvdetect: connect auth: connection has not been authorized
42610:dvdetect: The NDMP connection is not successfully
authorized on host 'storage_node_name'
```

To resolve this issue, relaunch the **Configure All Libraries** wizard and correct the NDMP username and password combination.

#### Note

If the **Log** window reports that NetWorker cannot detect the serial numbers for the library, see [Configuring an NDMP autochanger the jbconfig command on page 566](#) for detailed instructions.

## Configuring an NDMP autochanger the jbconfig command

The NMC interface is the preferred method to configure an NDMP autochanger. Use the jbconfig command when you cannot configure the autochanger by using the NMC Configure Library wizard.

The *EMC NetWorker Command Reference Guide* or the UNIX man page provides more information about the jbconfig command.

### Procedure

1. Login to the NetWorker server as root (UNIX) or Administrator (Windows).
2. At the command prompt, type the following command:  
`jbconfig`
3. Type 3 at the **What kind of jukebox are you configuring** prompt, to configure an autodetected NDMP SCSI jukebox.
4. When prompted for an NDMP username, specify the NAS administrator account. If DinoStor Tape Server manages the jukebox, then specify the DinoStor account.
5. When prompted for an NDMP password, specify the NAS administrator password. If DinoStor manages the jukebox, then specify the DinoStor password.
6. When prompted for the NDMP Tape Server Name, specify the NAS filer hostname. If DinoStor manages the autochanger, then specify the DinoStor hostname.
7. In the **What name do you want to assign to this jukebox device** prompt, provide a name to identify the autochanger.
8. To enable auto-cleaning, accept the default value of **Yes**, otherwise type **No**.
9. In the **Is (any path of) any drive intended for NDMP use? (yes / no) [no]** prompt, type **Yes**.
10. In the **Is any drive going to have more than one path defined? (yes / no) [no]** prompt, type **No** if you will not configure shared devices. Type **yes** to configure shared drives. [DDS on NDMP nodes in a SAN environment on page 194](#) provides detailed information about dynamically sharing NDMP devices.
11. The jbconfig command prompts for the first pathname for the NDMP devices in the jukebox.
  - a. Specify the pathname in the following format:

`NDMP_tape_server_name:device_path`

where:

- *NDMP\_tape\_server\_name* is the hostname of the NDMP or DinoStor Tape Server.
  - *device\_path* is the first device path.  
For a NetApp device, do not type a slash before the device name. Although the jbconfig command completes without errors, the NetApp filer will not recognize the tape device or autochanger.
- b. At the **Is this device configured as NDMP** prompt, type **yes**.
  - c. Repeat step a and step b for all NDMP devices in the autochanger.
  - d. When prompted, assign a hardware ID.
  - e. To use DDS:
    - Respond to the prompts as required so that the first host will have access to the shared drive.

- When prompted to share this drive with another host, type **yes**
  - When prompted, type the hostname and device path of the second host that will have access to the shared drive.
12. Complete the prompts for the second device.
13. In the **Enter the drive type of drive 1** prompt, specify the number that corresponds to the NDMP device type.
14. If each drive in the autochanger is the same model, then type **yes**. Otherwise, type **no** then specify the appropriate device types for each additional autochanger device.
15. When prompted to configure another autochanger, type **no**.

## Changing the block size of an NDMP device

By default, the block size used to write data to an NDMP backup is 60KB. With the exception of EMC Celerra, when you specify the *NDMP\_AUTO\_BLOCK\_SIZE=Y* variable for an NDMP client, an NDMP device can use the value defined in its Device block size attribute.

[Table 104 on page 571](#) describes how to configure the *NDMP\_AUTO\_BLOCK\_SIZE* variable. Consult the applicable vendor documentation to determine the block sizes supported by the NDMP filer before setting the block size for an NDMP device.

To change the block size defined for the NDMP device, perform the following steps:

### Procedure

1. From the **View** menu, select **Diagnostic Mode**.
2. In the **Devices** window, right-click the NDMP device and select **Properties...**
3. On the **Advanced** tab, select a value in the **Device block size** field.
4. Select a supported value in the **Device block size** attribute. The selected block size must not exceed the block size configured on the NAS filer.
5. Click **Ok**.

## Configuring NDMP-DSA devices

When you use DSA, NetWorker sends the NDMP data to an AFTD. The steps to configure an AFTD for NDMP data and non-NDMP data are the same. [Advanced file type devices on page 157](#) provides detailed information.

The steps to configure an NDMP-DSA autochanger are the same as configuring a library for non-NDMP data. [Autodetection of libraries and tape devices on page 132](#) provides detailed information.

## Configuring the Clone Storage Node

When cloning NDMP data, specify the destination storage node, called the clone “write source” (the device that receives the clone data), in the Clone storage nodes attribute. Prior to NetWorker 8.0, the Client resource contained the Clone storage node attribute. In NetWorker 8.0 and later, the backup Storage Node resource contains this attribute. [Storage node selection criteria and settings for writing a clone on page 335](#) provides details.

## Creating resources to support NDMP clients

Before you configure resource such as a pool, group and schedule for the NDMP client, review the information in the following table.

**Table 102** NDMP resource requirements

| Resource | Resource requirements for NDMP                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |
|----------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Pool     | <p>When you create a pool for non-NDMP devices, select only the devices required for the NDMP clients.</p> <p>NetWorker cannot send bootstrap and index backups to an NDMP device. Configure a separate pool to direct the index and bootstrap to a non-NDMP device. <a href="#">Directing client file indexes and bootstrap to a separate media pool on page 286</a> provides more information.</p> <p>When you do not configure a non-NDMP devices or a non-NDMP device is not available to receive the index and bootstrap backups, the NDMP client backup appears to hang.</p> <p>Auto media verification does not support NDMP.</p> <p>When an NDMP client backup is a member of a clone-enabled group, configure a clone pool with non NDMP devices, local to the NetWorker server to receive the clone bootstrap and index.</p>                                                                                                                                                                                                                                                                                                                                          |
| Schedule | <p>NetWorker does not support the use of synthetic full backup levels for NDMP data. EMC Celerra, Isilon, VNX, and NetApp filers with NDMP version 4 or later support token-based backups (TBB) to perform NDMP full, incremental, and level 1-9 backups. NetWorker supports the same number of incremental levels that the NAS vendor supports. EMC Celerra, Isilon, and NetApp documentation provide the maximum number of incremental levels that the TBB incremental backup can support.</p> <p>When you configure TBB after you update the NetWorker server from 7.6 SP1 or earlier, the first incremental or level 1 to 9 backups does not occur until after one complete full backup.</p> <p>Filers that do not support TBB, do not support incremental backups. If you select the level incr, the NetWorker server performs a full backup. However, you can schedule level backups to function like incremental backups.</p> <p>For example, define a weekly backup schedule of full on day 1, level 1 on day 2, level 2 on day 3, level 3 on day 4, and so on.</p> <p>Verify the NAS storage vendor supports NDMP incremental backups before you use this feature.</p> |
| Group    | <p>For Direct-NDMP backups, set the Savegrp parallelism value to the number of available NDMP drives.</p> <p>If you set the Savegrp parallelism attribute to a higher value, there will not be enough drives to support all of the queued backup save sets. Large save sets might fail due to the inactivity timeout limit.</p> <p>When NDMP groups back up simultaneously, divide the number of drives by the number of groups. Use this value for each of the Savegrp parallelism attributes.</p> <p>Setting the Savegrp parallelism value for the group overrides the parallelism value defined for the NDMP clients.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    |

**Table 102** NDMP resource requirements (continued)

| Resource      | Resource requirements for NDMP                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              |
|---------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|               | To enable automatic cloning of NDMP data, enable the Clones checkbox under the Setup tab of the group properties window then select the appropriate clone pool.<br>For NetApp clients that will use checkpoint restart, set the value of the Client retries attribute under the Advanced tab to a number greater than 0.<br>With the exception of Isilon, NetApp, and EMC Celerra filers, when the Force Incremental attribute is set to Yes, and the Interval attribute is set to a value less than 24 hours, a level 1-9 backup is backed up at level Full.               |
| Browse policy | When you define the browse policy an NDMP client, consider the amount of disk space required for the client file index. NDMP clients with several thousand small files will have significantly larger client file indexes on the NetWorker server than a non-NDMP client. A long browse policy for an NDMP client will increase disk space requirements on the file system that contains the client file indexes. <a href="#">Setting up policies for quick access and long term storage on page 64</a> provides more details on configuring browse and retention policies. |

## Creating and configuring the NDMP client resource

Use the NMC Client Configuration Wizard to create the NDMP client or create the client manually. EMC recommends that you use the NMC Client Configuration Wizard to create NDMP clients.

### Using the Client Configuration wizard

Review this information before you use the NMC Client Configuration Wizard to create the NDMP client.

- For an NDMP configuration that includes storage node resources, configure a client resource for each storage node that you define for an NDMP backup and clone operation.
- For NDMP three-party storage nodes that use NDMP devices, repeat these steps for each NDMP storage node.
- For NDMP-DSA storage nodes, create the NetWorker client resources in the same manner as non-NDMP clients. [Creating a backup Client resource on page 65](#) provides details on how to create a non-NDMP client resource.

#### Procedure

1. From the **Administration** window in NMC, click **Configuration**.
2. In the expanded left pane, select **Clients** and then from the **Configuration** menu select **New > client wizard**.
3. In the **Client Name** field, specify the hostname of the filer.
  - For EMC Celerra, you will typically use the CIFS server name configured on the Data Mover.
  - For EMC Isilon, use a hostname associated with a non-aggregated (non-teamed) network connection to one of the Isilon cluster nodes that has a fixed IP address. Do not use the SmartConnect hostname.

4. Select **NDMP client** and then click **Next**.
5. In the **NDMP User Name** field, specify a valid NAS administrator account.
  - For an EMC Celerra and VNX filers, specify the trusted account that you create on each NDMP-Host Data Mover for backups. Some versions of EMC Celerra require you to use an account called **ndmp**. The *Configuring NDMP on EMC Celerra* document on the EMC Online Support web site provides more information.
  - For an Isilon, specify the username and password of an NDMP administrator. The *OnFS Users Guide* on EMC Online Support web site describes how to create NDMP administrators.
6. In the **NDMP Password** attribute, specify the password for the NAS administrator account, and then click **Next**.
 

[Troubleshooting NDMP configuration and backup failures on page 580](#) describes how to resolve errors that you may experience when you configure the NDMP client.
7. In the **NDMP backup type** attribute, select or specify the backup type. The following table summarizes the supported backup types for each NAS.

**Table 103** Supported backup types

| NAS                 | Supported backup types                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |
|---------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| EMC Celerra and VNX | <ul style="list-style-type: none"> <li>• tar</li> <li>• dump — traverses a file tree in mixed width first and depth-first order. The optimal backup type.</li> <li>• vbb — used to backup the entire volume at the block level rather than at a file level. The vbb backup type reads data blocks in a more efficient method compared to traditional file-based backups. The vbb backup type does not support DDAR, TBB, and Three party backups.</li> <li>• ts — enables a tape silervering backup.</li> </ul> |
| Isilon              | <ul style="list-style-type: none"> <li>• tar — use this backup type for Checkpoint Restart.</li> <li>• dump</li> </ul>                                                                                                                                                                                                                                                                                                                                                                                          |
| BlueArc             | <ul style="list-style-type: none"> <li>• dump</li> </ul>                                                                                                                                                                                                                                                                                                                                                                                                                                                        |
| MiraPoint           | <ul style="list-style-type: none"> <li>• image</li> </ul>                                                                                                                                                                                                                                                                                                                                                                                                                                                       |
| NetApp              | <ul style="list-style-type: none"> <li>• dump— an inode-based backup that traverses a file tree in directory first and file-based order.</li> <li>• smtapes—performs a block-level backup of a SnapMirror volume.</li> </ul>                                                                                                                                                                                                                                                                                    |

8. The **NDMP Array Name** field enables you to configure the same NAS device with multiple NDMP clients that have different host IDs, specify the logical name assigned to the NDMP NAS array.

#### Note

NDMP clients that use the same NAS device must have the same NDMP array name.

9. Review the **App Info** options and disable options, as required. EMC recommends that the default options remain enabled. The Online Wizard help describes each **App Info** option.

10. In the **Advanced App Info** field, specify additional NAS specific environments variables, one per line. The following table provides a list of the available **Application Information** environment variables for each NAS.

**NOTICE**

Environment variables are case-sensitive. Use an equal (=) sign to separate the environment variable name from its value.

**Table 104** Vendor-specific Application Information variables

| NAS                 | Variables                                              | Definition                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   |
|---------------------|--------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| EMC Celerra and VNX | <p><i>DIRECT=n</i></p> <p><i>EMC_EDIRnn=string</i></p> | <p>Optional. When you use DAR or DDAR, you must set this value to y.</p> <p>Optional. This string value identifies a directory to exclude from the backup. You can use asterisk (*) as a wildcard, but only when * is the last character in the string. To include multiple directories, increment the number.</p> <p>For example:</p> <ul style="list-style-type: none"> <li>• EMC_EDIR01=/fsX/DIRx</li> <li>• EMC_EDIR02=/fsX/DIRy</li> </ul> <p>EMC Dart version 5.5 and later supports this variable.</p> <p>This variable is ignored when you perform a vbb backup.</p> |
|                     | <i>EMC_EFILEnn=string</i>                              | <p>Optional. This string value determines which files to exclude from the backup. You can use the asterisk (*) as a wildcard, but only when * is the first or last character in the string, or both. To include multiple files, increment the number.</p> <p>For example:</p> <ul style="list-style-type: none"> <li>• EMC_EFILE01=*mp3</li> <li>• EMC_EFILE02=temp*</li> </ul> <p>EMC Dart version 5.5 and later supports this variable.</p> <p>This variable is ignored when you perform a vbb backup.</p>                                                                 |
|                     | <i>OPTIONS=NT</i>                                      | Required. This value ensures backup and recovery all ACLs. In addition to setting this variable, <i>axtrrp</i> must exist in the /nas/server/slot_#/netd file.                                                                                                                                                                                                                                                                                                                                                                                                               |

**Table 104** Vendor-specific Application Information variables (continued)

| NAS    | Variables                                                                                                                                              | Definition                                                                                                                                                                                                                                                                                                         |
|--------|--------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|        | <i>SNAPSURE=y</i>                                                                                                                                      | Required. This value ensures that NetWorker can back up open files and generate FH information.                                                                                                                                                                                                                    |
|        | <i>USE_TBB_IF_AVAILABLE=n</i>                                                                                                                          | Optional. The NetWorker software automatically enables TBB support for EMC Celerra filers. Specify this variable and value to disable TBB support for incremental backups and when you use the vbb backup type. When you specify this value, the backup reverts to the native level-based backup of the NAS.       |
|        | <i>ALLOW_SINGLE_FILE_BACKUP=y</i>                                                                                                                      | Optional. Specify this variable only when you perform a single file backup.                                                                                                                                                                                                                                        |
|        | <i>NSR_NDMP_RECOVER_NO_DAR=y</i>                                                                                                                       | Optional. Specify this variable to perform a non-DAR recovery when you set the <i>DIRECT=y</i> variable during the backup.                                                                                                                                                                                         |
|        | <i>NSR_NDMP_DDAR</i><br>This environment variable must be set in the operating system before invoking the either the recover or winworkr program.      | Optional. Specify this variable to perform a DDAR recovery when: <ul style="list-style-type: none"> <li>• You set the <i>DIRECT=y</i> variable during the backup</li> <li>• The DART version is 5.5 and later Do <i>not</i> specify <i>NSR_NDMP_DDAR</i> when you also use <i>NSR_NDMP_RECOVER_DIR</i>.</li> </ul> |
|        | <i>NSR_NDMP_RECOVER_DIR=y</i><br>This environment variable must be set in the operating system before invoking either the recover or winworkr program. | Optional. Specify this variable to perform a DAR recovery when: <ul style="list-style-type: none"> <li>• When you set the <i>DIRECT=y</i> variable during the backup</li> <li>• The DART version is 5.5 and later Do not use <i>NSR_NDMP_RECOVER_DIR</i> when you also use <i>NSR_NDMP_DDAR</i>.</li> </ul>        |
|        | <i>TS=y</i>                                                                                                                                            | Optional. Enables tape silvering.                                                                                                                                                                                                                                                                                  |
| Isilon | <i>DIRECT=y</i>                                                                                                                                        | Required.                                                                                                                                                                                                                                                                                                          |
|        | <i>HIST=F</i>                                                                                                                                          | Required for Checkpoint Restart backups to ensure the use of path based file history.                                                                                                                                                                                                                              |
|        | <i>FILES=pattern</i>                                                                                                                                   | Optional. Use this variable to back up only files that match the defined pattern. You can use wildcards in the pattern definition.                                                                                                                                                                                 |

**Table 104** Vendor-specific Application Information variables (continued)

| NAS    | Variables                        | Definition                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |
|--------|----------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|        | <i>PER_DIRECTORY_MATCHING=y</i>  | Optional. Use this variable along with the <i>FILES=pattern</i> variable. Matches the pattern defined by FILES across directories.                                                                                                                                                                                                                                                                                                                                              |
|        | <i>USE_TBB_IF_AVAILABLE=n</i>    | Optional. The NetWorker software automatically enables TBB for Isilon filers. Specify this variable to disable TBB support for incremental backups and when you use the vbb backup type. When you specify this value, the backup reverts to the native level-based backup of the NAS.                                                                                                                                                                                           |
|        | <i>NSR_NDMP_RECOVER_NO_DAR=y</i> | Optional. Define this variable to perform a non-DAR recovery when you set the DIRECT=y variable during the backup.                                                                                                                                                                                                                                                                                                                                                              |
|        | <i>NDMP_AUTO_BLOCK_SIZE=Y</i>    | Optional. Specify this variable to override the default block size of 60 KB when writing NDMP backups to an NDMP device. Uses the block size value defined in the Device block size attribute when you labeled the NDMP volume. <a href="#">Configuring NDMP devices on page 563</a> provides more information.                                                                                                                                                                 |
| NetApp | <i>FILESYSTEM=path</i>           | Optional. Use this variable to define the file system to back up and override the value in the Save set attribute of the client.                                                                                                                                                                                                                                                                                                                                                |
|        | <i>DIRECT=y/n</i>                | Optional. When you use DAR or DDAR, you must set this value to y.                                                                                                                                                                                                                                                                                                                                                                                                               |
|        | <i>EXCLUDE=string</i>            | Optional. This string specifies files to exclude from backup. The following rules apply: <ul style="list-style-type: none"> <li>The string must be a file name. Use file names, not absolute paths.</li> <li>You can use the asterisk (*) as a wildcard, only when * is the first or last character in the string, or both.</li> <li>To list multiple files, separate each name with a comma. A comma cannot appear as part of the file name. You cannot use spaces.</li> </ul> |

**Table 104** Vendor-specific Application Information variables (continued)

| NAS | Variables                       | Definition                                                                                                                                                                                                                                                                                                                    |
|-----|---------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|     |                                 | <ul style="list-style-type: none"> <li>You can specify up to 32 strings.</li> </ul>                                                                                                                                                                                                                                           |
|     | <i>EXTRACT_ACL=y</i>            | Optional. Specify this variable to recover ACLs when you use DAR.                                                                                                                                                                                                                                                             |
|     | <i>SMTAPE_BREAK_MIRROR=Y</i>    | Optional when you use SMTape. During the recovery of the mirror, setting <i>SMTAPE_BREAK_MIRROR=Y</i> ensures that the mirror breaks and the volume becomes available for reuse. If you do not set the variable or you specify <i>SMTAPE_BREAK_MIRROR=N</i> , the mirror remains in the same state as at the time of backup.  |
|     | <i>SMTAPE_DELETE_SNAPSHOT=Y</i> | Optional when you use SMTape. When backing up the filer volumes, setting <i>SMTAPE_DELETE_SNAPSHOT=Y</i> ensures the removal of the mirror created during the backup, at the end of backup. If you do not set the variable or you specify <i>SMTAPE_BREAK_MIRROR=N</i> , each backup attempt creates a new snap mirror image. |
|     | <i>RECURSIVE=y</i>              | Optional for DAR and DDAR recoveries. <i>RECURSIVE=y</i> ensures the correct recovery of ACLs, permissions, and ownerships for all interim directories selected in the recover operation.                                                                                                                                     |
|     | <i>RECOVER_FULL_PATHS=y</i>     | Optional for DAR and DDAR recoveries. <i>RECOVER_FULL_PATHS=y</i> ensures the NetWorker recovers the ACLs, permissions, and ownerships for each interim directories selected in the recover operation.                                                                                                                        |
|     | <i>USE_TBB_IF_AVAILABLE=n</i>   | Optional. The NetWorker software enables TBB automatically. Specify this variable to disable TBB support for incremental backups and when you use the vbb backup type. This value reverts the backup to the native level-based backup of the NAS                                                                              |
|     | <i>UTF8=n</i>                   | Optional. Provides support for UTF-8 formatted data. When you do not define this variable, the default value is n.                                                                                                                                                                                                            |

**Table 104** Vendor-specific Application Information variables (continued)

| NAS       | Variables                             | Definition                                                                                                                                                                                                                                   |
|-----------|---------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|           |                                       | When you set <i>UTF8=Y</i> during an NDMP client backup and the backup contains path names with non-ASCII characters, an index-based recovery of this backup fails with the error:<br><br>"RESTORE: could not create path pathname"<br><br>. |
|           | <i>NSR_NDMP_RECOVER_NO_DAR=y</i>      | Optional. Specify this variable to perform a non-DAR recovery when you set the <i>DIRECT=y</i> variable during the backup.                                                                                                                   |
|           | <i>NDMP_AUTO_BLOCK_SIZE=Y</i>         | Optional. Specify this variable to override the default block size of 60 KB when writing NDMP backups to an NDMP device. Uses the block size value defined in the Device block size attribute when you labeled the NDMP volume.              |
| Mirapoint | <i>MIRA_OPTIONS= (fromimagefull=)</i> | Required. The <i>(fromimagefull=)</i> value allows full image and message (file) based backups to use the date of the image when performing the selection.                                                                                   |
|           | <i>NDMP_AUTO_BLOCK_SIZE=Y</i>         | Optional. Specify this variable to override the default block size of 60 KB when writing NDMP backups to an NDMP device. Uses the block size value defined in the Device block size attribute when you labeled the NDMP volume.              |
| BlueArc   | <i>NDMP_BLUEARC_FH_NAMETYPE=UNIX</i>  | Required. This variable requests that the BlueArc filer provide UNIX-style names when backing up a CIFS share.                                                                                                                               |
|           | <i>NDMP_AUTO_BLOCK_SIZE=Y</i>         | Optional. Specify this variable to override the default block size of 60 KB when writing NDMP backups to an NDMP device. Uses the block size value defined in the Device block size attribute when you labeled the NDMP volume.              |

11. On the **Specify the Client Backup Options** window:

- To enable DSA backups, select **DSA Backup**.
- In the **Target Pool** field, select the pool that will receive the client data.

- c. If you use Data Domain devices, then select **Data Domain Backup**.
- d. For NetApp and Isilon filers only:
  - To configure NetWorker to restart a scheduled NDMP backup that fails, select the option **Checkpoint enabled**. [Checkpoint restart backups on page 92](#) provides more information about checkpoint restart backups.
  - To decrease the frequency checkpoints written during an NDMP backup, increase the **Checkpoint Granularity (in bytes)** value to 5.
- e. Click **Next**.

12. Select or specify the objects to backup:

- When the NAS supports NDMP snapshot management extension, you can browse and mark individual file systems to back up. When the client supports browsing, by default, NetWorker selects all objects.
- When the client does not support browsing, specify the save sets to back up.
  - To back up all of the file systems on the client, type ALL.
  - NAS versions earlier than 3 do not support the ALL save set. List the file systems one per line.
  - When you do not use the ALL save set, specify the file system name, as configured on the NAS.
  - File system names in the save set field are case sensitive.
  - For EMC Celerra backups, do not use the ALL save set. List the file systems, one per line excluding the root, or “/” file system. When you include the root file system, client index updates fail for hidden file systems (directories that start with a “.”) with the error: Failed to store index entries.
  - For EMC Celerra block-level backups, specify the entire file system mount point.
  - You cannot specify a share name.

13. To back up large client file systems, optionally schedule each file system to back up separately. For example, create two separate clients with the same name, but with different save sets.

14. Select the **Browse Policy** and **Retention Policy** for the NDMP client.

15. In the **Remote Access** attribute:

- Specify the root (on UNIX) or administrator (on Windows) account of any computer that you use to browse entries for the NDMP computer.  
For an Isilon filer in SmartLock compliance mode, specify the compadmin account.
- Specify the NetWorker server administrator account (Windows) or the root account (UNIX).

Use this format to specify each account:

```
account_name@hostname
```

16. Click **Next**.

17. On the **Choose the Backup Group** window:

- To add the client to an existing group, select **Add to an existing group** then select the group name.
- To create a new group:
  - Select **Create a new group**.

- For NetApp clients that will use checkpoint restart, set the value of the Client retries attribute to a number greater than 0.
- In the Schedule Backup Start Time, specify the time to start the group backup.
- Select Automatically start the backup at the schedule time.

18.On the **Specify Storage Node options** window:

- To use NDMP devices managed by the NetWorker server, select **Backup to NetWorker server only**.
- To backup to a remote storage node, select **Backup to the Following storage nodes**.

19.On the **Backup Configuration Summary** window, review the attributes and click **Create**.

20.Review the configuration summary then click **Create**.

21.Click **Finish** to exit the wizard.

## Performing post Client Configuration Wizard steps

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

### Modifying the client parallelism

On the **Globals (1 of 2)** tab, modify the client parallelism value to the recommended value for the NDMP configuration.

- For Direct-NDMP, set the **Parallelism** attribute to 1.
- For NDMP-DSA, the parallelism value depends on the NAS capabilities and you must set parallelism to a value that is appropriate for the NAS. Parallelism values of 4 to 8 are common. In general, the optimal parallelism setting depends on filer configuration and the amount of installed RAM.
- For an EMC Celerra and VNX filers, the parallelism value differs for the DartOS version:
  - For an EMC Celerra using DartOS v.5 and earlier, the **Parallelism** attribute cannot exceed 4. *Configuring NDMP Backups on EMC Celerra* provides more information.
  - For VNX using DartOS v.6 and later, the maximum parallelism value is 8. The optimal parallelism value depends on:
    - The amount of physical memory on the Data Mover.
    - The amount of physical memory allocated to the NDMP PAX configuration.
    - The value defined for the *concurrentDataStream* parameter on the filer. *Configuring NDMP Backups on VNX* provides more information.
- For a NetApp filer, the recommended parallelism value is 8. If required, you can use a higher parallelism value however, for best performance, do not exceed 12.

### Modifying the Storage Node

On the **Globals (2 of 2)** tab, specify the appropriate storage node in the **Storage Nodes** attribute.

The attribute value depends on the type of backup:

- When you perform Direct-NDMP backups with NDMP devices, specify the hostname of the NAS that manages the tape device or autochanger.
- For three-party backups, list the destination host first.

- For NDMP-DSA backups, specify the hostname of the storage node that manages the tape device or autochanger. If the NetWorker server is the storage node, specify `nsrserverhost`.
- For a DinoStor-managed NAS, specify the hostname of the DinoStor server first.

**NOTICE**

In NetWorker 8.0 SP1 and later, for NDMP-DSA backups, the NetWorker software uses the Storage Node attribute field of the NDMP client to determine which host receives the backup data. The `nsrndmp_save` command does not require the `-M` and `-P` options. If you specify the `-M` and `-P` options, they will override the **Storage Node** attribute value.

---

## Configuring the NDMP client manually

EMC recommends that you create a new NDMP client by using the Client Configuration Wizard. If you create the NDMP client manually, then the configuration details for each attribute in the Client Configuration Wizard apply when you create the client manually.

Review this information before you configure an NDMP client manually.

- NDMP does not support the use of directives including AES encryption. The NetWorker software ignores any value you define in the Directives attribute for an NDMP client.
- When you select Checkpoint enabled on the General tab, do not modify the Checkpoint granularity attribute. NDMP backups do not support checkpoint granularity and the NetWorker software ignores any value that you define for this attribute.
- In NetWorker 8.0 and later, if the NAS supports NDMP snapshot management extension, then you can browse and mark individual filesystems for backup instead of specifying the save sets in the Save Set attribute. You cannot use the Save set browse icon to browse the NDMP file system until you:
  - Select the NDMP checkbox, on the **Apps & Modules** tab.
  - Specify the NDMP username and password in the Remote user and password fields on the **Apps and Modules** tab.

## Performing NDMP backups

After you configure the NetWorker server for NDMP backup data operations, you can perform scheduled or manual NDMP backups.

The steps to configure a scheduled NDMP backup are the same as configuring non-NDMP scheduled backups.

On Windows, you can manually back up NDMP data by using the NetWorker User program. The method to backup NDMP data is the same as a non-NDMP local backup. [Performing a manual backup on Windows on page 71](#) provides more information.

**NOTICE**


---

You cannot perform a three-party backup with the NetWorker User program.

---

On Windows and UNIX you can perform a manual backup from a command prompt by using the `nsrndmp_save` command. [Performing an NDMP backup from the command line on page 579](#) provides more information.

Before performing a manual backup by using the `nsrndmp_save` command or the NetWorker User program, review these requirements:

- You can only perform manual Direct-NDMP backups from a NetWorker server.
- You can start a manual NDMP-DSA backups from a NetWorker server, storage node, or client. When you do not start the NDMP-DSA backup from the NetWorker server, the servers file on the NetWorker server and storage node, must contain the hostname of the host that initiates the backup.
- Before you perform a manual backup, you must configure the NDMP client on the NetWorker server. Manual backups use client configuration information for example, the variables defined in the Application Information attribute of an NDMP client.
- Direct-NDMP and three-party NDMP backups support manual DAR backups when the NDMP client contains the `DIRECT=Y` and `HST=Y` environment variables in the Application Information attribute for the NDMP client.

#### NOTICE

To use DAR, the NAS filer must use NDMP version 4. The *EMC NetWorker Software Compatibility Guides* describes how to determine if a particular NDMP vendor supports DAR.

---

## Performing an NDMP backup from the command line

Use the `nsrndmp_save` command to perform a manual command line NDMP backup.

The `nsrndmp_save` command does not back up the bootstrap. Without the bootstrap, you cannot perform a disaster recovery of the NetWorker server. To back up the bootstrap, run the `savegrp -G group_name` command from the NetWorker server. The `savegrp` command uses the attribute values specified for the group. For example, the pool and schedule values.

To perform an NDMP backup from the command prompt, use the following syntax.

```
nsrndmp_save -T backup_type -s NetWorker_servername -c clientname -l
backup_level -t date_time -g savegroup path
```

where:

- *backup\_type* is a supported backup type for the NAS filer:
  - NetApp supports the `dump` and `smtape` backup types.
  - The optimal backup type for the EMC Celerra NAS is `tar` or `dump`. Use the `vbb` backup type to back up the entire volume at the block level.
  - Isilon supports the `dump` and `tar` backup types
  - BlueArc only supports the `dump` backup type.
  - MiraPoint only supports the `image` backup type.
- *backup\_level* is the full for a full backup, `incr` for an incremental backup, or the appropriate backup level in the range 1-9. Each NAS supports full and level 1-9 backups. EMC Celerra, Isilon, and NetApp filers only support incremental level backups.
- *date\_time* is the date and time of the last backup, enclosed in double quotes. You must specify this value for `incr` level backups, but not for level 1-9 backups. When you do not specify the date and time, the backup is a native NDMP level-based backup.

**NOTICE**

During a NetWorker scheduled group backup, the NetWorker software supplies the date and the time information, and incremental and level backups work as expected.

Use one of the these methods to determine the date and time of the last NDMP backup:

- Review the `daemon.raw` file on the NetWorker server or the `savegroup` completion report for a line similar to the following:

```
42920:nsrndmp_save: browsable savetime=1296694621
```

Use the value after `savetime=` with the `-t` option.

- Specify the date and time of the last backup reported by the `mminfo` command for the NDMP save set.

## Example of a NDMP backup

To perform an incremental backup of a NetApp client named `mynetapp`, perform the following steps.

1. Determine the time of the last full backup:

```
mminfo -v -c mynetapp
```

| client   | date     | time     | size   | ssid       | fl   | lvl  | name      |
|----------|----------|----------|--------|------------|------|------|-----------|
| mynetapp | 02/16/11 | 15:23:58 | 1853MB | 3864812701 | cbNs | full | /.../set1 |
| mynetapp | 02/17/11 | 15:39:58 | 815MB  | 3848036430 | cbNs | incr | /.../set2 |

2. Specify the last backup time in `nsrndmp_save` command:

```
nsrndmp_save -T dump -s my_nwserver -c mynetapp -l incr -t
"02/16/11 15:23:58" -g mygroup path
```

In NetWorker 8.0 SP1 and later, for NDMP-DSA backups, the NetWorker software uses the Storage Node attribute field of the NDMP client to determine which host receives the backup data. The `nsrndmp_save` command does not require the `-M` and `-P` options. If you specify the `-M` and `-P` options, they will override the **Storage Node** attribute value. The *EMC NetWorker Command Reference Guide* and the `nsrndmp_save` man page on UNIX provide more information.

## Troubleshooting NDMP configuration and backup failures

This section provides a list of the possible causes and the resolutions for NDMP backup failures.

### Unable to connect to NDMP host *hostname*

This message appears when the NetWorker server cannot create or modify an NDMP client.

To resolve this issue ensure that the environment meets the following requirements:

- Username and password specified for the client is correct and has sufficient permissions to perform NDMP operations.

- NDMP service is running on the filer.

## NetWorker features not supported on NetApp NDMP v3 and earlier

Features such as Checkpoint restart require NDMP v4.

To verify the NDMP version, perform the following steps.

1. Log in to the NetApp host as root or as a Windows Administrator.
2. Display the NDMP version:

```
ndmpd version
```

To change the NDMP version:

1. Log in to the NetApp host as root or as Windows Administrator.
2. Stop the **NDMP** process:

```
ndmpd off
```

3. Change the **NDMP** version:

```
ndmpd version 4
```

4. Restart the **NDMP** process:

```
ndmpd on
```

## Cannot perform NDMP backup after the NetWorker server licenses expire

If a NetWorker sever running in evaluation mode expires before you authorize the server, NDMP devices remain disabled after the addition of the required licenses and authorization of the NetWorker server.

To re-enable NDMP devices, perform the following steps.

1. Use NMC to connect to the NetWorker server and click the **Devices** button.
2. In the **Devices** windows, right-click the NDMP device and select **Properties**.
3. Click the **Configuration** tab and set the **Target Sessions** attribute to 1.
4. Click the **General** tab and in the **Enabled** section, select **Yes**.
5. Click **Ok**.

## No PAX threads available

This error message appears in the `server_log` on the NDMP Data Server when the client parallelism value for an EMC Celerra client exceeds what the EMC Celerra can support.

To resolve this issue adjust the client parallelism attribute to a value that the Celerra supports:

- For an EMC Celerra client that runs DartOS v5.0 or earlier, the client parallelism value cannot exceed 4.
- For an EMC Celerra client that runs DartOS v6.0, the maximum parallelism value supported is 8, or the value defined in the `concurrentDataStreams` variable on the EMC Celerra. By default, the `concurrentDataStreams` variable is 4.
- The maximum parallelism value also depends on the available physical memory and the amount of memory allocated to the PAX configuration. Configuring NDMP Backups on EMC Celerra on the EMC Online Support web site provides more information.

## Failed to store index entries

This error message occurs in the daemon.raw file when an index backups fails due to an insufficient amount of swap space.

To resolve this issue, increase the amount of swap space available to the NetWorker server.

**NOTICE**

You cannot use the NetWorker User program to perform file-by-file and save set recoveries from a backup when the corresponding index update failed.

---

## IO\_WritePage write failed - No space left on device (28): No space left on device

This error message appears in the daemon.raw file when the index backup fails. There is insufficient temporary space to store the index entries before the NetWorker software commits the information into the client file index.

To resolve this issue, specify a new the temp directory with sufficient disk space in one of the following ways:

- Define the NSR\_NDMP\_TMP\_DIR environment variable in the Application Information attribute of the client.
- Define the NSR\_NDMP\_TMP\_DIR as an operating system environment variable on the NetWorker server.

[Memory and space requirements for NDMP FH updates on page 560](#) describes how to determine the amount of disk space the NetWorker software requires to temporarily store client files index entries.

**NOTICE**

You cannot use the NetWorker User program to perform file-by-file and save set recoveries from a backup when the corresponding index update failed.

---

## Error reading the FH entries from save through stdin

This error message appears in the daemon.raw file of the NetWorker server when there is a communication error between nsrndmp\_save and nsrndmp\_2fh processes.

Resolve any communication or connection issues, then retry the backup.

**NOTICE**

You cannot use the NetWorker User program to perform file-by-file and save set recoveries from a backup when the corresponding index update failed. [Performing an NDMP save set recovery from the command prompt on page 594](#) describes how to use a save set recover to restore the data.

---

## Cannot find file history info for filename...You may still be able to recover this file with a saveset recovery

This error message appears in the daemon.raw file of the NetWorker server when FH information is missing or corrupted for the file specified in the error message. For example, NetWorker cannot update the client file index(CFI) with FH information when a

backup process interruption occurs during the failover of a clustered NetWorker environment.

You cannot perform an NDMP file-by-file recover or a save set recover when the CFI does not contain the associated FH information.

To recover this file, perform a save set recover from the command prompt. [Performing an NDMP save set recovery from the command prompt on page 594](#) provides for further information.

#### NOTICE

The NetWorker server does not delete the FH files stored in the tmp directory when the CFI updates fail.

---

## **nsrndmp\_save: data connect: failed to establish connection**

This error message appears in the daemon.raw file of the NetWorker server for several reasons:

- Network connectivity or name resolution issues exist between the NetWorker server and the NDMP client.
- You specified an incorrect NDMP username or password specified for the NDMP client.
- The NDMP service is not started on the NAS filer.
- The NetWorker server cannot communicate with the NAS filer over port 10000.
- A free port in the NetWorker server's default port range (7937-9936) is not available during an NDMP-DSA backup.  
EMC NetWorker Security Configuration Guide provides more information about NDMP port requirements and configuration.
- A misconfigured loop router. For an EMC Celerra filer, the server route command utility configures the loop router. For NetApp, the route utility configures loop back router. The value of this setup is network-specific and depends on the number of switches and hubs between the NAS filer, NetWorker server, and NetWorker storage node.
- On the host where DSA is running, if the hostname is present in the hosts file, the nsrdsa\_save process uses this name during backup. The DSA host passes the loopback entry to the NDMP data server and the connection fails. To resolve this issue, remove the hostname from the localhost list.

Knowledge base article esg11713 on the EMC Online Support Site provides detailed troubleshooting information for this error message and other failed to establish connection failures encountered during an NDMP backup.

## **nsrndmp\_save: get extension list: communication failure**

This message appears during a NDMP local backup when NetWorker cannot determine the filer name.

To resolve this issue, perform the following steps.

1. From a command prompt on the NetWorker server, type: **nsrndmupsup -c NDMP\_hostname -o output\_filename**  
For example:

```
nsrndmupsup -c myfiler.mnd.com -o nsrndmupsup.txt
```

2. Edit the output file that the **nsrndmupsup** command generates and search for the string **Vendor Name**. Make note of the reported Vendor Name.

For example:

```
Vendor Name = BlueArc Corp
```

3. Change to the /nsr/debug directory on UNIX or the NetWorker\_installation\_dir\nsr\debug directory on Windows.
4. Create new empty file and name it with the following format:

```
ndmpgettextlist_disable_VENDOR_NAME
```

where you replace VENDOR\_NAME with the vendor name of the filer reported in the nsrndmps output file.

For example, to create this file for a BlueArc filer on UNIX, type:

```
touch "ndmpgettextlist_disable_BluArc Corp"
```

## Cloning NDMP save sets

You can clone Direct-NDMP and NDMP-DSA save sets by using the same methods used to clone non-NDMP save sets.

- [Creating resources to support NDMP clients on page 568](#). describes how to configure automatic cloning of NDMP data immediately after a group backup.
- [Cloning on page 319](#) provides information on other cloning methods.

Before you clone NDMP save sets, review these requirements:

- To clone Direct-NDMP or Three-party backup data:
  - The source NAS must run NDMP version 3 or later.
  - The destination NAS can run any version of NDMP, but you cannot clone a volume cloned with NDMP earlier than version 3 to another volume.
  - You cannot clone NDMP save sets to a non-NDMP device.
  - You can clone NDMP tapes from one NDMP host to another NDMP host of the same type. For example, you can clone tapes from a NetApp filer with an attached library to another NetApp filer or to the same filer.
- You require two NDMP devices to clone the NDMP save sets, one device to perform the read operation and one device to perform the write operation.
- A scheduled or automatic clone operation clones the index and bootstrap save sets. You must have a non-NDMP device available to receive the cloned copy of the index and bootstrap backups. This non-NDMP device is in addition to the non-NDMP device that contains the source bootstrap and index backup. When you manually clone NDMP data, the clone operation does not clone the bootstrap and index data.
- You must clone NDMP-DSA backups to non-NDMP devices. You can however, clone NDMP-DSA save from one type of tape device to another. For example you can clone save sets on a DLT device to an AIT device.
- Use the nsrclone program to clone NDMP save sets from a command prompt. The *EMC NetWorker Command Reference Guide* or the UNIX man pages provide more information on nsrclone usage.

# Reporting NDMP Data

The NetWorker software reports information about NDMP clients, data, and volumes in two ways.

- The NMC reporting feature—Reports NDMP data in the same manner as non-NDMP data. Refer to [Enterprise reporting and events monitoring on page 389](#) provides more information.
- The `mminfo` command. Use the `mminfo` program to query the media database for NDMP volume or save set information.

## Querying the NDMP volumes by backup type with the `mminfo` command

You can query save sets by backup format (NDMP or DSA) to display volume information.

- For example, to query NDMP volumes, type `mminfo -q ndmp`. Output similar to the following appears:

| volume   | client    | date      | size    | level | name |
|----------|-----------|-----------|---------|-------|------|
| 005D0000 | sim1cifs1 | 6/22/2011 | 1036 MB | full  | /fs1 |
| 005D0001 | sim1cifs1 | 6/22/2011 | 173 MB  | full  | /fs1 |
| 005D0001 | sim1cifs1 | 6/22/2011 | 862 MB  | full  | /fs1 |
| 005D0002 | sim1cifs1 | 6/22/2011 | 348 MB  | full  | /fs1 |

- For example, to query NDMP -DSA volumes, type `mminfo -q dsa`. Output similar to the following appears:

| volume   | client      | date       | size   | level | name      |
|----------|-------------|------------|--------|-------|-----------|
| NDMP.001 | 10.8.67.219 | 12/13/2011 | 644 MB | full  | /vol/vol0 |
| NDMP.001 | 10.8.67.219 | 12/13/2011 | 402 MB | full  | /vol/vol1 |
| NDMP.001 | 10.8.67.219 | 12/13/2011 | 402 MB | full  | /vol/vol1 |
| NDMP.001 | 10.8.67.219 | 12/13/2011 | 36 MB  | full  | /vol/vol2 |

## Querying the NDMP save sets with the `mminfo` command

Query the media database to determine which save sets are NDMP save sets and the status of an NDMP save set in the media database. NDMP save set status information is important when performing NDMP recoveries.

- To perform a browseable NDMP recover, the `ssflags (fl)` field for an NDMP save set must contain a `b`. The `b` value denotes a brows able save set.
- To perform a save set recover from the NetWorker User program, the `ssflags (fl)` field for an NDMP save set must contain a `b`.
- An NDMP save set contains an `N` attribute in the `ssflags (fl)` field.
- An NDMP-DSA save set contains an `s` attribute in the `ssflags (fl)` field.

In the following example, the NDMP save set status is recoverable (`r`). To recover the data, you can only perform a save set recovery from a command line.

| volume | type | client | date      | time    | size   | ssid       | fl  |
|--------|------|--------|-----------|---------|--------|------------|-----|
| vol1   | dlt  | clnt   | 6/22/2011 | 3:15:12 | 1036MB | 3842140553 | hrN |

In the following example, the NDMP-DSA save set status is browsable (b). Recover the data by using the NetWorker User program, or from the command line. A browseable NDMP-DSA save set supports browsable and save set recoveries.

```
mminfo -av
volume type client date time size ssid fl
lvl name
vol1 dlt clnt 6/22/2011 3:15:12 36MB 4259813785 cbNs
full /fs1
```

## Performing NDMP recoveries

NetWorker uses the `nsrndmp_recover` program to coordinate recover operations between the NetWorker software and the NDMP client. The `nsrndmp_recover` program does not move data to the NDMP client. When the `nsrndmp_recover` program identifies an NDMP-DSA save set, `nsrndmp_recover` automatically invokes the `nsrdsa_recover` program on the same host that runs the `nsrndmp_recover` command.

To recover NDMP data, you can run the `nsrndmp_recover` program from a command prompt, or use one of following programs, which automatically start the `nsrndmp_recover`:

- `recover`—The command line program on Windows and UNIX.
- `winworkr`—The NetWorker User GUI on Windows.
- The NMC Recovery Wizard. [Using the Recovery Wizard on page 353](#) describes how to use the Wizard to recover data.

During the recovery process, the `nsrndmp_recover` program passes nlist information to the NDMP client. There are three methods to recover NDMP backups:

- Index-based file-by-file recover — The nlist includes file offset and ACL information. When you recover many files, the recover process uses a significant amount of system resources on both the NetWorker server and the NDMP client to build and process the nlist information.
- Full save set recovery—The nlist only includes the path to the recovery directory, down to and including the mount point. When you recover many files, the recover process uses less system resource intensive than an index-based NDMP recover to build and process the nlist information.
- NDMP directory restore — A partial save set recovery of a single file or single directory.

For example, when the NetWorker software writes NDMP data to a remote storage node, start the recover program on the NetWorker storage node to prevent the data from traversing the network.

---

### Note

When you start the recover program on the NetWorker server, the data flows from the storage node to the NetWorker server and from the NetWorker server to the NDMP client, over the network.

---

## NDMP recovery requirements

The following table summarizes the requirements for each recovery feature.

**Table 105** Requirements of each NDMP recovery feature

| Feature                   |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |
|---------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| scanner                   | You cannot use the scanner command with the -i, -f and -r options on an NDMP volume. You cannot use the scanner command on a volume that contains NDMP and non-NDMP save sets when you load the volume in an NDMP device. The <i>Scanner command usage</i> technical note provides more information about using the scanner command with NDMP data.                                                                                                                                                                                                                                                                                                                                                                                  |
| Cross platform recoveries | You can recover NDMP data to different NDMP client however, you cannot perform a cross platform recover. Recover NDMP data to an NDMP client that is the same brand, a compatible model, and the same operating system as the original NDMP client.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |
| Devices                   | Recover Direct-NDMP and Three-party backups performed to an NDMP device from an NDMP device. To improve recover performance from an NDMP tape device, configure the tape device to support variable length records.<br>Recover NDMP-DSA backups from a non-NDMP device.                                                                                                                                                                                                                                                                                                                                                                                                                                                              |
| Localized environments    | When recovering data in a localized NDMP environment, the Index Recover status window shows the process in English and not the localized language.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   |
| NDMP-DSA                  | For better recovery performance, start the recover process on the NetWorker host where the backup volume resides.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    |
| Immediate recoveries      | Run the <code>nsrndmp_recover</code> program on the storage node with the locally attached backup device to perform an immediate recovery of NDMP-DSA data.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |
| EMC Celerra and VNX       | During recover operation the filer skips char and block special files. The following error message appears:<br><br><code>Warning: /fs1/SPE_REL/my.char_file has an unknown file type, skipping</code><br><br>When you recover named pipes: <ul style="list-style-type: none"> <li>• If the recover directory contains 10,000 or more named pipes, then the recover will fail. Ensure that the recover directory contains less than 10,000 named pipes.</li> <li>• The recover process changes the file permissions. The NetWorker software recovers named pipes as normal files.</li> </ul><br>The <i>Configuring NDMP for VNX</i> on EMC Online Support describes how to recover a tape silvering backup to a different data mover. |
| Blue Arc                  | The recover process creates a <code>\$__NDMP__</code> directory at the root level of the recovery file system when you recover more than 1,024 files. The directory contains the file list that the NetWorker server uses for an index recovery. Do not change the directory and its contents during an active recovery operation. When a recovery is not in progress, you can delete the directory.<br>While performing NDMP backup and recover operations, a message similar to the following may appear:<br><code>NDMP session—Unknown environment variable name ignored.</code>                                                                                                                                                  |

**Table 105** Requirements of each NDMP recovery feature (continued)

| Feature   |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    |
|-----------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|           | You can ignore this message.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |
| Mirapoint | After a full backup recovery for a Mirapoint system, reboot the Mirapoint system. An incremental recovery does not require a reboot.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |
| vbb       | <p>When you set backup type for an EMC Celerra or VNX filer to vbb, the NetWorker software performs a block-based backup. The NetWorker software recovers the data to a raw device. Use the Relocate data option to specify the raw device.</p> <p>When you use deduplication on the source or target file system, you cannot perform an index based file-by-file recover.</p> <p>When you perform a destructive save set recover, the recover process performs the following actions:</p> <ul style="list-style-type: none"> <li>• Recovers the data to the original location or an alternate location.</li> <li>• Overwrites existing data.</li> <li>• Overlays the data at the file system level and reimposes the saved image on the file system.</li> </ul> <p><i>Configuring NDMP backups on Celerra and Using Celerra Data Deduplication on EMC Support Online</i> provides detailed information about how to prepare the filer before you perform FDR.</p> |

## DAR and DDAR

By default, the NDMP recover process reads an entire tape from start to finish. The recover process extracts the data as it encounters the data on the tape. For large backup images, recovery is slow.

The DAR/DDAR recovery process:

- Provides the ability to recover a file or directory from the exact location on a tape.
  - Only passes the directory path to the NAS filer.
  - Reduces the size of the nlist information that the recover process stores in memory. During the recover process, the NAS filer assumes that the directory path includes all cataloged files and directories.
  - Does not sequentially read the file or record numbers on the tape to locate the data. This reduces the amount of time you require to recover specific files from a backup.
- EMC Celerra with DART version 5.5 and later and NetApp filer with NDMP v4 and OnTap version 6.4 and later support DDAR.

### Note

[Creating and configuring the NDMP client resource on page 569](#) describes how to configure the DAR and DDAR Application Information attributes for NDMP clients.

Use the `recover` command or the NetWorker User program to perform DAR and DDAR recoveries. You cannot use the `nsrndmp_recover` program to perform DAR/DDAR recoveries.

### When not to use DAR or DDAR

The DAR and DDAR recoveries send multiple path names across the network to the NDMP Data Server and, in three-party configurations, to the NetWorker server. The recover

process stores the path names in memory on the NDMP Data Server. Recoveries of a large amount of data from a large save set can negatively impact the network and the NDMP Data Server resources.

Do not use DAR and DDAR to recover the following objects:

- Several thousands of files in a single index-based recover operation.
- A specific directory structure containing several thousand or millions of files.

To perform a non-DAR-based recovery of a save set when you set the *DIRECT=y* at the time of backup, first define the *NSR\_NDMP\_RECOVER\_NO\_DAR=y* variable in the Application Information attribute of the NDMP client.

## Performing an NDMP index-based file-by-file data recovery

Perform an NDMP index based file-by-file recover in the same manner as a non-NDMP data recover. You can restore the data to the original NDMP client or directed to a different NDMP client.

Before you perform an index-based file-by-file recover, review the following information.

- Set the *HIST=y* in the Application Information attribute of the NDMP client at the time of the backup. [Table 104 on page 571](#) provides more information about the NDMP Application Information attributes.
- The NDMP save set must be browsable. You cannot perform a browsable recover of a recoverable or recyclable save set. [Reporting NDMP Data on page 585](#) describes how to determine the status of an NDMP save set.
- Do not use an index-based recovery to recover a large numbers of files or directories. For better recovery performance, use a save set recover. [Performing a full or Directory Restore of NDMP data by using a save set recovery on page 592](#) provides more information.
- To perform an index-based file-by-file recover:
  - Use the NetWorker User program on a Windows host. [Performing an NDMP index-based file-by-file recover using the NetWorker User program on page 589](#) provides detailed information.
  - Use the **recover** program. [Performing an NDMP index-based file-by-file recover from a command prompt on page 591](#) provides detailed information.

### Performing an NDMP index-based file-by-file recover using the NetWorker User program

On Windows, to recover data to the original NDMP client or to a different NDMP client, perform the following steps.

#### Procedure

1. Open the NetWorker User program and connect to the NetWorker server.

#### **NOTICE**

If you receive the error

```
No file indexes were found for client client_name on server server_name.
Try connecting to a different NetWorker server
```

and you selected the correct NetWorker server, then ensure that you selected a browsable save set. Alternatively, perform a save set recover. [Performing an NDMP save set recovery from the command prompt on page 594](#) describes how to perform an NDMP save set recover from a command prompt.

2. Select **Recover** to open the **Source Client** window.
3. Select source NDMP client and click **OK**. The local client is the default selection.
4. Select the destination client for the recovered data and click **OK**. If the destination client is not the source client, ensure the NAS filer is the same brand, a compatible model and the same operating system as the source NDMP client.
5. Optionally, recover the data from an earlier backup time. The **Recover** window appears with the latest version of the backup files. To recover data from an earlier backup, change the date and time of backup using one of the following methods:
  - a. Change the browse time for all files in the recover window:
    - From the **View** menu, select **Change Browse Time**.
    - In the **Change Browse Time** window, select a new day within the calendar. Select **Previous Month** or **Next Month** to change from the current month.
    - In the **Time** field, change the time of day by typing an hour, a minute, and the letter a for A.M. or p for P.M. Use the 12-hour format.
    - Click **OK**.
  - b. View all versions of the selected file system object:
    - Highlight the file or directory for review.
    - From the **View** menu select **Versions**.
    - Once you locate the version to recover, change the browse time. To change the browse time, highlight the volume, directory, or file and click **Change Browse Time**. The **Version** window closes and the **Recover** window reflects the new browse time.
6. Optionally, search for the files. To search for and recover the most recently backed-up version of a file or directory:
  - a. From the **File** menu, select **Find**.
  - b. Type the name of the file or directory. Use wildcards to expand the search; without wildcards, partial filenames do not provide any results.
7. Mark the data to recover. To select file system objects to recover:
  - a. In the left pane of the **Recover** window, click the appropriate directory folder.
  - b. Mark each directory or file to recover by selecting the checkbox next to each directory or file.
8. Optionally, relocate the data to a different location. By default, the recover process recovers the selected files to the original location.

**NOTICE**

NDMP recoveries will always overwrite existing files. EMC recommends that you recover the NDMP data to a different location, to avoid data loss.

---

To relocate the files to a different location:

- a. Select **Recover Options** from the **Options** menu.

NDMP recovery do not support the following options:

- Rename recovered file
- Discard recovered file
- Prompt for every file conflict

NDMP recoveries will *always* overwrite existing files. EMC recommends that you relocate the NDMP data to a different location, to avoid loss.

- b. In the **Relocate Recovered Data To** field, type the full pathname of the target directory, click **OK**.

The target directory is a literal string and *must* match the path as seen by the NAS filer in its native OS, exactly. Otherwise, the recover process uses the original location and overwrites existing files with the same name.

9. Optionally, to view the volumes required to recover the marked file system objects, from the **View** menu, select **Required Volumes**.

10. Click **Start** to begin the recovery. If any required volume is not available to the NetWorker server, a volume status warning appears.

When this warning appears:

- a. Click **No**.
- b. From the **View** menu, select **Required Volumes**.
- c. Ensure that the NetWorker software can mount each listed volumes in an available device.
- d. Attempt the recover operation again.

The NetWorker server takes a few moments to recover the files, depending on file size, network traffic, server load, and tape positioning. During this time, messages appear so that you can monitor the progress of the recovery.

When the recovery completes successfully, a message similar to the following appears:

```
Received 1 file(S) from NSR server server
Recover completion time: Tue Jan 21 08:33:04 2009
```

## Performing an NDMP index-based file-by-file recover from a command prompt

This section applies to command line recoveries from a Windows and UNIX client.

To avoid using the Windows version of `recover.exe` on Windows operating systems, perform one of the following actions:

- Specify the full path to the `recover` program. For example: `C:\Program Files\EMC NetWorker\nsr\bin\recover.exe`.
- Ensure that the `$PATH` environment variable contains the `NetWorker_install_path\bin` directory before `%SystemRoot%\System32`.

To recover NDMP data from a command prompt on a UNIX or Windows NetWorker host, perform the following steps:

### Procedure

1. From the command prompt, type:

```
recover -s NetWorker_servername -c client_name
```

where:

- the `-s NetWorker_servername` option specifies a particular NetWorker server on the network to use when recovering data.

When you do not use the `-s` option, the `recover` program tries to connect to the first computer listed in the `servers` file. When the `servers` file does not contain any

servers, or lists more than one server, the **Change Server** window appears, and you can select the server.

- the **-cclient\_name** option specifies the source NDMP client.
2. When prompted, type the directory to browse, for example:

```
cd /mydirectory
```

3. Use the **add** command to add the required files or folders to the recover list. The *EMC NetWorker 8.0 Command Reference Guide* provides a complete list of options for the **recover** command.
4. When restoring NDMP data, EMC recommends that you relocate the NDMP data to a different location. The NDMP protocol does not allow you to handle naming conflicts. The **recover** operation overwrites existing files with the same name.

- To relocate the data to a different directory, type:

```
relocate destination_directory_name
```

The target pathname for **destination\_directory\_name** is a literal string and must match the path as seen by the NAS filer in its native OS, exactly. Otherwise, the **recover** operation uses the original location and overwrites existing files with the same name.

- To recover the data to a different host, type:

```
relocate target_hostname::/mount_point
```

Data ONTAP may require you to add a backslash (\) after the mount point. For example, **target\_hostname::\mount\_point\**.

5. After you add all of the required files, type:

```
recover
```

## Performing a full or Directory Restore of NDMP data by using a save set recovery

You perform an NDMP save set recover in the same manner as a non-NDMP save set recovery. You can recover data to the original NDMP client or directed the data to a different NDMP client of the same platform.

Before you perform a full save set recover, review the following information:

- Use a full save set recovery to recover all files and folders in an NDMP data save set or to recover an entire directory within an NDMP save set. You cannot use the NetWorker User program to perform an NDMP Directory Restore. [Performing an NDMP save set recovery from the command prompt on page 594](#) provides more information.
- To use the NetWorker User program on Windows, a client file index entry for the save set must exist. When the index entry for the save set does not exist, the recover fails with an **index not found** error. When the client file index entries do not exist for the save set, use the **nsrndmp\_recover** program with the '**-v off**' option. [Performing an NDMP save set recovery from the command prompt on page 594](#) provides more information.
- You cannot perform a save set recover from the NetWorker User program when the save set status is eligible for recycling (E). The recover process requires a recoverable (r) or browsable (b) save set status.
  - [Reporting NDMP Data on page 585](#) describes how to determine the status of an NDMP save set.

- [Recovering a save set entry into the client file index and media database on page 374](#) describes how to change the status of a save set.
- A save set recover reads the entire tape set, from beginning to end, to find and recover the requested files. The recovery process completes when the recover operations reads all required tapes in their entirety.
- As each file recovers, the file name appears on the target share but the file size is 0 KB. The actual file size update occurs after the recovery completes.
- The following sections describe how to perform a full save set recover:
  - [Performing an NDMP save set recover by using the NetWorker User in Windows on page 593](#) describes how to recover data from a Windows host by using the NetWorker User program.
  - [Performing an NDMP save set recovery from the command prompt on page 594](#) describes how to recover NDMP data from a command prompt on Windows and UNIX hosts.
  - [Performing destructive save set recoveries for vbb backups on page 595](#) describes how to use the `nsrndmp_recover` program on Windows and UNIX hosts to recover from a vbb backup.

## Performing an NDMP save set recover by using the NetWorker User in Windows

### **NOTICE**

When the recover operations fails with the error: “Failed to propagate handle <number> to child process: Access is denied” the save set is not in the client file index of the NDMP client. Perform a save set recover from a command prompt. [Performing an NDMP save set recovery from the command prompt on page 594](#). provides more information.

### Procedure

1. Start the NetWorker User program.
2. On the **Change Server** window, select the NetWorker server and click **Ok**.
3. Select **Options > Recover Save Sets**.
4. On the **Source Client** window, select the appropriate NDMP client and click **Ok**.
5. On the **Save Sets** window, select the name of the save set.
6. Select the version of the save set, if there are multiple versions. You can also select the cloned version of a save set, if applicable.
7. To recover specific files and directories instead of the entire save set:
  - a. Click **Files**.
  - b. Specify the files and directories, one per line.
  - c. Click **OK**.

### **NOTICE**

Do not use this method to mark tens of thousands of files. Instead, use perform an NDMP Directory Restore. Marking many files and directories generates a large nlist and requires intensive resources on both the NetWorker server and the NAS filer.

8. Click **Recover Options**.

An NDMP data recovery does not support the following options:

- Rename recovered file
- Discard recovered file
- Prompt for every file conflict

**NOTICE**

EMC recommends that you relocate the NDMP data to a different location. NDMP recoveries *always* overwrite existing files.

9. To recover the data to a pathname that is different from the original backup location, in the **Relocate Recovered Data To** field, type the full pathname of the destination directory, then click **Ok**.

For NDMP data recoveries, the target pathname is a literal string and *must* exactly match the path as seen by the native OS on the NAS filer. Otherwise, the recover operation uses the original location and overwrites existing files with the same name.

- Use the **Relocate recovered data to this raw device** option when performing a SnapImage destructive restore. The *NetWorker SnapImage Module 2.5 Solaris Version Installation and Administration Guide* and the *NetWorker SnapImage Module 2.5 Windows Version Installation and Administration Guide* provides more information.

10. To recover the data to a different NDMP client, specify the name of the client to receive the NDMP data in the **Destination Client** field.

11. To view the volumes required to perform the recover, select **View > Required Volumes**

12. Click **OK** to begin the recovery. The recovery status appears in the **Recover Status** window.

## Performing an NDMP save set recovery from the command prompt

To perform a save set recovery to the original NDMP client or to a different NDMP client, use the nsrndmp\_recover command.

For example:

```
nsrndmp_recover -s NetWorker_server -c source_ndmp_client -S ssid/
cloneid -v off -m target_ndmp_client:::/target_path /source_path
```

where:

- *source\_ndmp\_client* is the hostname of the source NDMP client.
- *target\_ndmp\_client* is the hostname of the destination NDMP client.
- */source\_path* is the original location of the data.
- */target\_path* is the location to recover the data.

**NOTICE**

EMC recommends that you relocate the NDMP data to a different location. NDMP recoveries always overwrite existing files. The */target\_path* is a literal string and must exactly match the path as seen native OS on the NAS filer. Otherwise, the recover operation uses the original location and overwrites existing files with the same name.

- **-v off** allows you to restore data when client file index of the NDMP client does not contain information about the NDMP save set.  
In the following examples, the NetWorker server is mars and the backup client is venus.

- To recover a mount point `/mnt` from a backup of NDMP host venus to a directory `/newmnt` on NDMP host jupiter, type:

```
nsrndmp_recover -s mars -c venus -S 123456789 -v off -m
jupiter:::/newmnt
```

- To recover a mount point `/mnt` from a backup of NDMP host venus to NDMP host pluto, type:

```
nsrndmp_recover -s mars -c venus -R pluto -S 123456789 -v off -
m /mnt
```

Data ONTAP may require you to add a slash (/) after the mount point. For example, `target_hostname::/mount_point/`.

## Performing destructive save set recoveries for vbb backups

Use the `nsrndmp_recover` command with the `-r raw_device` and `-m mount_point` options to perform a destructive save set recovery.

### NOTICE

Do not perform a NDMP Directory Restore from a vbb backup of a Celerra deduplicated file system.

For example:

On a Microsoft Windows system to perform a destructive save set recovery to the `/data` drive:

```
nsrndmp_recover -s mars -c venus -m /data -r raw_device_name -S
2674606849
```

On a UNIX system, the following command performs a destructive save set recovery to the `/dev/c1t1d0s0` device, mounted at the `/` file system:

```
nsrndmp_recover -s mars -c venus -r /dev/c1t1d0s0 -S 2674606849 -m /
```

The *EMC NetWorker Command Reference Guide* or the UNIX man page provides more information about the `nsrndmp_recover` command.

If you do not specify the `-r` option when you use the `-m`, the recover operation:

- Is nondestructive.
- Operates at the file or directory level, rather than the file system level.

This nondestructive restore overwrites existing files on the destination that have the same names as those in the recovery list. Other data remains untouched on the file system.

Use this nondestructive method to:

- Perform a directory level recovery on a high density file system.
- Recover many files in one directory.

## Troubleshooting NDMP recover

This section provides a list of the possible causes and the possible resolutions for NDMP recovery issues.

## RESTORE: could not create path *pathname*

This error message appears when restoring NetApp data. This error, when encountered, appears in the `daemon.raw` file of the NetWorker server and the recovery output.

To resolve this issue:

- Ensure that you specify a source and a target path during the recover that exists on the target filer.
- If you set the `UTF8=Y` application information variable during an NDMP client backup and the backup contains path names with non-ASCII characters, then perform a save set recover. Index-based recoveries will fail with this error message.

## These files were not restored (Restore failed with error, or file/directory specified but not found in backup)

This error message appears in the `daemon.raw` file of the NetWorker server and the in the recovery output.

To resolve this issue:

- Ensure that the file or directory specified during the recover, exists in the save set.
- Ensure the pathname specified to relocate the data exists on the destination filer. For NDMP data recoveries, the target pathname is a literal string and must exactly match the path as seen by the native OS on the NAS filer.

# CHAPTER 22

## SNMP Module

This chapter contains the following topics:

- [SNMP traps](#)..... 598
- [Configuring NetWorker SNMP notifications](#)..... 598
- [Configuring SNMP management software](#)..... 600

## SNMP traps

The NetWorker Simple Network Management Protocol (SNMP) Module allows NetWorker servers to send notification messages to SNMP management agents.

You must configure SNMP-enabled network management software to accept traps from the NetWorker server. For detailed information about SNMP management operations refer to your network management documentation.

The NetWorker SNMP Module uses traps to communicate NetWorker event notifications to SNMP management stations. A trap is an unsolicited notification sent from the SNMP agent (the NetWorker server) to the SNMP event manager.

When you configure the SNMP notification in NetWorker, you can define the types of traps that the NetWorker server sends to the SNMP even manager. Typical traps include warnings, critical errors, and other messages from the NetWorker server.

## Configuring NetWorker SNMP notifications

The NetWorker software provides notifications to a variety of resources about NetWorker server events. The NetWorker SNMP Module is one of those resources. The module uses the `nsrtrap` program to forward notifications to the SNMP management software. When you configure the SNMP notification, you include the IP address or hostname of the SNMP management server, and other `nsrtrap` command line options, for example, the SNMP community and the trap type.

Before you configure the NetWorker SNMP notification, you must first license the NetWorker SNMP module. Contact EMC Licensing for more information.

### Command line options for nsrtrap

The NetWorker SNMP Module uses the `nsrtrap` program to send SNMP traps from the NetWorker server to the SNMP management software. The following table lists the command line options that you can include in the Action attribute when you configure the SNMP notification.

**Table 106** Command-line options for nsrtrap

| Option                    | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     |
|---------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <code>-c community</code> | Specifies the SNMP community that is authorized to receive traps from the NetWorker server. You configure SNMP communities on the SNMP server. The default setting for this option is Public, which means that the public community can receive traps from the NetWorker server. For security purposes, system administrators often customize the SNMP server to limit the communities that can accept traps. If the SNMP server configuration specifies a community other than Public, specify the appropriate community name. |
| <code>-t trap_type</code> | Optional, sets the type of trap that the NetWorker SNMP Module sends to the SNMP server. The default setting is 6, which sets the trap type to “enterprise-specific” and is the correct type for the notifications (error messages) that the NetWorker server sends to the SNMP server. Only modify the trap type if you intend to send a specific trap to the SNMP server and not a NetWorker notification.                                                                                                                    |

**Table 106** Command-line options for nsrtrap (continued)

| Option                                 | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             |
|----------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <code>-s<br/>specific_trap_type</code> | <p>Allows you to customize the identity of the type of trap that the NetWorker server sends. Set this option to any integer value. Use this option in conjunction with different SNMP notifications to distinguish different traps from the NetWorker server.</p> <p>For example, you can create separate SNMP notifications for critical messages, warnings, and events or priorities then use the <code>-s</code> option with a unique number to differentiate the various notifications. The Action attribute for each notification appears as follows:</p> <ul style="list-style-type: none"> <li>• Critical notification: <code>nsrtrap -s 1 SNMP_server_host_name</code></li> <li>• Warning notification: <code>nsrtrap -s 2 SNMP_server_host_name</code></li> <li>• Event or priorities notification: <code>nsrtrap -s 3 SNMP_server_host_name</code></li> </ul> <p>Configure the SNMP management software to recognize that NetWorker traps with the specific trap type of 1 are critical messages, trap type 2 are warning messages and trap type 3 are event or priority messages. Additional SNMP notifications can have other settings for the <code>-s</code> option to further differentiate various traps from the NetWorker server.</p> |
| <code>-v</code>                        | Sets the output mode to verbose. When you run <code>nsrtrap</code> from the command line in verbose mode, the program displays the community, trap type, specific trap type, and the hostname or IP address.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |

## Modifying preconfigured NetWorker SNMP notification

The NetWorker server has a preconfigured SNMP notification that you can modify.

### Procedure

1. Use NMC to connect to the NetWorker server.
2. In the **Administration** window, click **Configuration**.
3. Select **Notifications**.
4. Right-click **SNMP notification request** and select **Properties**.
5. In the **Action** attribute, specify the options for the `nsrtrap` command:

```
nsrtrap -c community_name -t trap_type -s specific_trap_type
SNMP_server_name
```

---

### Note

The `-s` and `-t` options are optional.

6. Click **OK**.

---

### Note

You cannot modify the event and priorities attributes for a preconfigured SNMP notification.

## Creating NetWorker SNMP notifications

### Procedure

1. Use NMC to connect to the NetWorker server.
  2. In the **Administration** window, click **Configuration**.
  3. Right-click **Notifications** and select **New**.
  4. Enter a name for the SNMP notification.
  5. (Optional) In the **Comment** attribute, enter a description of the notification.
  6. Select the events and priorities that the notification should communicate to your SNMP server.
- 

### Note

You cannot modify the events and priorities after you create the notification.

7. In the **Action** attribute, specify the options for the **nsrtrap** command:

```
nsrtrap -c community_name -t trap_type -s specific_trap_type
SNMP_server_name
```

---

### Note

The **-s** and **-t** options are optional.

8. Click **OK**.

## Configuring SNMP management software

You must configure the SNMP management software to recognize and accept traps sent by NetWorker servers.

For specific instructions that describe how to configure the types of acceptable traps in the SNMP management software, refer to the SNMP management software documentation.

## NetWorker SMI Network Management Private Enterprise Code

When you configure the SNMP management software to accept traps, you must indicate the specific trap type. Use the Structure of Management Information (SMI) Network Management Private Enterprise Code that applies to the specific network application that will send traps to the software. The Private Enterprise Code for the NetWorker server is 160. The complete code is .1.3.6.1.4.1.160.

## Receiving traps in the SNMP network management software

After you configure the SNMP network management software to accept traps from NetWorker servers, an icon for each NetWorker server appears on the network management console.

You can configure the SNMP network management software in the following ways:

- To indicate that a trap was received. For example, the NetWorker server icon may blink or change color.

- To track pending, alert, and other configured messages.
- To separate traps into event categories, such as Error Events, Status Events, Threshold Events, Configuration Events, Application Alert Events, or All Events. For information on how to set up SNMP trap templates, refer to the network management software documentation.



# CHAPTER 23

## DiskXtender Data Manager File System Support

This chapter contains the following topics:

- [Supported configurations](#).....604
- [DiskXtender Data Manager file system overview](#).....604
- [Backup of DXDM file systems](#).....606
- [Recovery of DXDM file systems](#).....608

## Supported configurations

These configurations are supported for the backup and recovery of DiskXtender Data Manager (DXDM) file systems:

- DXDM software and NetWorker server, client, or storage node software installed on the same computer.
- DXDM software installed on a computer that is a client of a computer that is running NetWorker server, client, or storage node software.

**NOTICE**

The Archive feature does not work for DXDM file systems.

---

The *EMC NetWorker Software Compatibility Guide* provides information about supported operating systems and file systems.

## Path information

NetWorker backup and recovery requires the /etc/dxuldm.path file when supporting a DXDM file system. The file is automatically created during DXDM installation.

## Permissions

The NetWorker daemon nsreexecd controls automated backup and recovery of DXDM file systems. The daemon is configured to run with set user ID (suid) root permissions. Root permissions are also required to perform manual NetWorker backup and recovery operations with DXDM file systems.

## DiskXtender Data Manager file system overview

DXDM file systems use the following enhancements that are not found in standard file systems:

- The creation and retention of DMAPI information for each file.
- The ability to migrate files to a storage target.
- The ability to purge file data from the file system after migration.
- The retention of a data stub for each purged file.

Through these enhancements DXDM provides file system access to large numbers of files while storing the bulk of the file data on one or more storage target systems.

## File data in a DXDM file system

When a file is placed into a DXDM file system it is available to list, view, access, and change the same as in any standard UNIX file system. The difference is that as soon as a file is placed into a DXDM file system, DMAPI metadata is created for the file. This extended metadata permits the transparent archiving of the file's data outside of the file system.

Some of the DMAPI information that is tracked on each file includes:

- The file's migration status.
- The file's purge status.

- The file's data stub size.

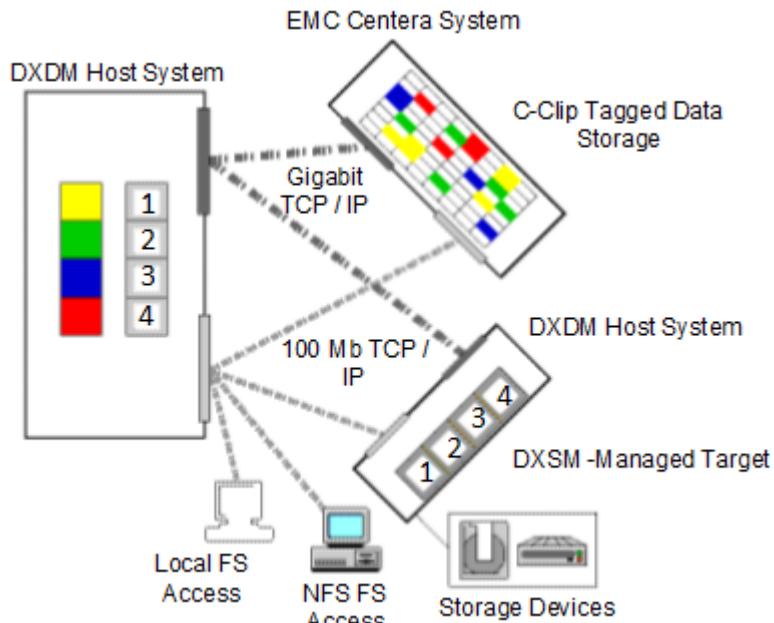
After a period of time the file's data is migrated to a storage target. The storage target can be a DXSM system or an EMC Centera Storage System (EMC Centera). After a file's data is migrated it exists on both the DXDM file system and the storage target.

After a period of time, unchanged files are purged from the file system. The file system retains the file's DMAPI metadata and data stub. The data stub consists of a user-configured number of bytes from the beginning of the file.

## User access to file data

The following figure depicts eight DXDM file systems on one host system. Four of the file systems use a DXSM storage target and four use a EMC Centera target.

**Figure 38** Prototypical DXDM installation



The diagram shows that the data from each DXDM file system exists in its own namespace on the storage target.

- On a DXSM storage target, relative pathnames and capabilities are used to identify files.
- On a EMC Centera storage target, the EMC C-Clip™ data is created to identify each file.

This storage target namespace information is not required by DXDM file system users for access to the files. Users need only know the full pathname of a file on the DXDM host system or, when access is provided over NFS, its relative pathname from the file system's NFS mount point.

When a file on a DXDM file system is changed it is marked as not migrated. Any previously migrated data for the changed file is retained on the storage target but renamed with a version label. When a file is deleted from a DXDM file system it is fully removed. Any previously migrated data is retained on the storage target and renamed with a version label and a deleted label.

## Backup of DXDM file systems

A DXDM file system consists of files and metadata. The files can be in a variety of migration and purge states. The metadata is contained in the file system's DMAPI attributes file. The following table shows the types of files and metadata that can exist in a DXDM file system and notes the types that are included in a NetWorker backup.

**Table 107** DXDM file system data types included in a NetWorker backup

| Data type                                                       | Included         |
|-----------------------------------------------------------------|------------------|
| New files which have not been migrated.                         | Yes              |
| Changed files which have not been migrated since being changed. | Yes              |
| Files which have been migrated but not purged.                  | Yes              |
| Data stubs for files which have been migrated and purged.       | Yes              |
| File data which exists only on a storage target system.         | No               |
| DMAPI metadata.                                                 | Yes <sup>a</sup> |

- a. The DMAPI metadata is included by default. It can safely be excluded. [Excluding the DMAPI attributes file on page 606](#) provides more information.

File data that has not changed since being migrated is protected by the storage target. NetWorker backup automatically excludes this data from its client/save sets when the data has been purged. This results in these benefits:

- Smaller client/save sets.  
Purged data which is protected on the storage target is excluded from the client/save set. This is normally the bulk of the data in a DXDM file system.
- Much faster backups.  
In addition to the time savings derived from the smaller client/save set, NetWorker backup prevents the lengthy process of retrieving purged file data from the storage target.

DXDM file system client/save sets should exclude the DMAPI metadata. [Excluding the DMAPI attributes file on page 606](#) provides more information.

Backups of a DXDM file system are performed in the same manner as backups of a standard file system. Backups can be performed on a scheduled basis or manually. Both methods require root permissions.

## Excluding the DMAPI attributes file

Every DXDM file system has a DMAPI attributes file which stores volatile DMAPI metadata. This file does not need to be backed up because it is re-created during the recovery process. Since these files can become quite large, create a global Directive resource to simplify the exclusion process.

To exclude a DMAPI attributes file:

### Procedure

1. Create a global Directive resource which excludes .DMATTR files. DXDM stores DMAPI attribute information in files located at the top level of each file system. The filename for these files is .DMATTR.

2. When creating the global Directive resource, use the Application Specific Module named Skip to exclude .DMATTR files. [Directives on page 269](#) provides more information on directives.
3. Apply the **Directive** resource when creating client/save sets for the file system.

## Aborted backups

A DMAPI process is initiated whenever a backup of a DXDM file system occurs. DXDM assigns a DMAPI session label of DXULDMLIB to this type of process. At the conclusion of a successful backup the process is removed.

If a backup is aborted, the DXULDMLIB process exists as a defunct process. Defunct DXULDMLIB processes exist as process table entries and use no system resources. These processes normally do not cause problems and are removed when the system is rebooted. However, they can be removed manually. [Removing a defunct DXULDMLIB process on page 607](#) provides details. [Viewing existing DMAPI processes on page 607](#) provides information on how to determine whether a defunct DXULDMLIB process exists.

## Viewing existing DMAPI processes

To view all DMAPI processes on a DXDM host system:

### Procedure

1. Log in as root on the DXDM host system.
2. Create the DXDM environment.

Use the correct command and file for the current shell:

- C shell (csh):

```
source /opt/dxuldm/etc/dxuldm.login
```

where /opt/dxuldm is the full path to the DXDM installation directory.

- Korn shell (ksh) or Bourne shell (sh):

```
. /opt/dxuldm/etc/dxuldm.profile
```

where /opt/dxuldm is the full path to the DXDM installation directory.

3. Type the **prtmdsession** command:

**prtmdsession**

The prtmdsession command lists each existing DMAPI session.

## Removing a defunct DXULDMLIB process

### NOTICE

Do not remove active DMAPI sessions. If active sessions are removed, DXDM processes terminate and file system activity is blocked until those processes are restarted.

### Procedure

1. Log in as root on the DXDM host system.
2. Create the DXDM environment. [Viewing existing DMAPI processes on page 607](#) provides details.
3. Type the **prtmdsession** command.
4. Find the listing which has **DXULDMLIB** in the **Session Info** field and note the integer in the listing's Session ID field.

5. Type the `deldm session` command:

```
deldm session -s DXULDMLIB -i session-id -n
```

where session-id is the integer from the defunct DXULDMLIB process's Session ID field.

## Recovery of DXDM file systems

Recovery of a DXDM file system consists of restoring data from a client save set and synchronizing the file system's DMAPI information with the data on the storage target.

### About recoveries

Recovery of backed-up data from a DXDM file system is performed by using the same procedures that are used for a standard file system. [Recovering Filesystem Data on page 347](#) provides details. DXDM file system recovery can consist of individual files, directories, or a file system.

With DXDM file systems, file data must be recovered into the same file system from which it is backed up. Attempting to recover backed up data into a new file system causes:

- The unavailability of all data on the storage target.
- The DXDM processes to stop responding.

This requirement is based on the nature of the DMAPI metadata that DXDM file systems use to locate and access data on the storage target. The DMAPI metadata uses full pathnames. If the file-system mount point changes because of a recovery into a new file system, the pathname information in the metadata becomes inaccurate.

### Recovered files list

As part of the recovery process each restored file's pathname is listed in a file on the DXDM host system. DXDM uses this information to synchronize its metadata. [File system synchronization on page 609](#) provides details.

When a recovery is complete, all data in the file system is available without waiting for the synchronization process. Data on the storage target becomes available after synchronization.

This data requires synchronization:

- Migrated and purged file data.
- Purged and deleted file data. [Restoring deleted files and previous file versions on page 608](#) provides details.

## Restoring deleted files and previous file versions

DXDM file systems retain file versions. This allows administrators to restore specific versions of files. In a DXDM file system, a file is migrated when it is first placed into the file system and again after each change. Each of these migrations cause a new version of the file to be created on the storage target.

To restore a previous version of a file, whether or not the file still exists in the file system:

### Procedure

1. Recover the file from the client/save set that backed up the desired version. [Recovering the data on page 352](#) provides information on this procedure.
2. Complete the synchronization process. [File system synchronization on page 609](#) provides details.

3. To expedite the synchronization of a particular file, complete the procedure described in [Manually synchronizing a file on page 610](#).

### Results

The synchronization process restores the data for the version of the file that is recovered. It will also restore data for a file which has been inadvertently deleted. At the conclusion of the synchronization process the recovered file version or deleted file is available.

## File system synchronization

As part of a recovery of one or more files into a DXDM file system, the recover program creates a file that contains a list of each recovered file.

This list file has a pathname with this format:

/opt/dxuldm/adm/readdir/rec.date.pid

where:

- /opt/dxuldm is the installation directory for DXDM.
- date is the date of the recovery.
- pid is the process ID of the NetWorker client process.

DXDM uses the list file to rebuild the file system's DMAPI attributes file. This process synchronizes the file system's metadata with the data on the storage target.

#### **NOTICE**

Do not remove a list file created by the recover program. Automatic file synchronization will not occur if a list file is removed.

Manual synchronization can be conducted without a list file. [Manually synchronizing a file on page 610](#) provides more information. [Automatic synchronization on page 609](#) describes that synchronization is an automatic process which does not require administrative intervention.

[Manually synchronizing a file on page 610](#) describes how make a file's data available more quickly.

If NetWorker recover cannot write to the readdir directory, each recovered file is synchronized as it is recovered. This file-by-file synchronization significantly slows down the recovery process.

The readdir directory is created during the installation of DXDM. NetWorker recover will be unable to write to it if the directory is removed or if the partition on which it is mounted becomes full.

## Automatic synchronization

DXDM uses the list file created by NetWorker recover to determine which files require synchronization. Each file on the list is synchronized. If synchronization does not complete, DXDM retries until all files on the list have been synchronized. After all files are synchronized, the list file is removed.

Automatic synchronization is performed by the script dxuldmcronscript which is invoked by root's crontab every 10 minutes. The cron job to invoke dxuldmcronscript is placed in root's crontab when DXDM is installed.

## Manually synchronizing a file

To make a file available before automatic synchronization is complete, use manual synchronization. This uses the DXDM command-line utility dxuldmrecover.

### Procedure

1. Log in as root on the DXDM host system.
2. Create the DXDM environment. Step 2 in [Viewing existing DMAPI processes on page 607](#) provides details.
3. Run the **dxuldmrecover** utility:

### Results

```
dxuldmrecover -p filepath
```

where `filepath` is the full path to the file that is being synchronized.

The `dxuldmrecover` utility takes the full path of a file as its argument. It can be invoked from a script to manually synchronize multiple files.

When synchronization is complete this message appears:

```
Successfully recovered file filepath.
```

---

### Note

A DXDM file system can be manually synchronized by using the `dxuldmrecoverfs` utility. The *EMC DiskXtender Data Manager, Release 2.6, Installation and Administrator's Guide* provides more information.

---

# CHAPTER 24

## Windows Bare Metal Recovery

This chapter contains the following topics:

- [Terminology](#)..... 612
- [Overview of Windows Bare Metal Recovery \(BMR\)](#)..... 613
- [Windows BMR Planning](#)..... 620
- [Performing a Windows BMR backup](#)..... 628
- [Performing a Windows BMR recovery to physical or virtual computers](#)..... 632

# Terminology

The following list provides a description of typical Windows BMR backup and recovery terminology. The roadmap indicates which steps you need to perform before you attempt a Windows BMR recovery.

This chapter uses the following terms to describe NetWorker support for Windows BMR technology:

## Bare Metal Recovery (BMR)

The operation that restores the operating system and data on a host after a catastrophic failure, such as a hard disk failure or the corruption of critical operating system components. A BMR is an automated process that does not require the manual installation of an operating system. NetWorker provides an automated BMR solution for Windows that uses the Windows ASR writer and other Microsoft VSS writers to identify critical volumes and perform a full recovery on a disabled computer.

## Offline recovery

A restore operation performed from the NetWorker Windows BMR boot image. A BMR recovery is an offline recovery. You cannot select specific files or save sets to recover during an offline recovery. You must perform an offline recover to the same or similar hardware.

## Online recovery

A restore operation performed from the NetWorker User interface or recover command. An online recovery requires you to boot the computer from an installed operating system and enables you to recover only specific files or save sets. The topic *Recovering file system data* provides more information about online recoveries.

## Application data

User data that an application creates, such as log files or a database. For example, the application data of a SQL server includes databases and log files. You cannot use Windows BMR to recover the application data. You must back up and recover application data with NetWorker Module for Microsoft (NMM).

## ASR writer

The Volume Shadow Copy Service (VSS) writer that identifies the critical data that NetWorker must back up to perform an offline recovery.

## Boot Configuration Data (BCD)

A data store that contains a description of the boot applications and boot application settings that start the Microsoft Windows operating system. To perform an offline recovery, you must back up this ASR writer component.

## Critical volume

One of the following:

- Any volume that contains files for an installed service. The volume can be mounted as an NTFS directory. Exchange 2010 is an example of an installed service, but the Exchange database and log files are not considered critical.
- Any parent volume with a mounted critical volume.

### NOTICE

NetWorker considers all volumes on all dynamic disks critical if at least one of the volumes is critical.

---

A Windows BMR recovery requires a current backup of all critical volumes.

## Recovery

The restoration of the operating system and data for a host after a catastrophic failure, such as a hard disk failure or the corruption of critical operating system components. The recovery operation might be an offline recovery (Windows BMR) or an online recovery.

## NetWorker Windows BMR image

A bootable image that contains the NetWorker binaries and a wizard to control the Windows BMR recovery process.

## Non-critical volume

A volume that contains user data and does not contain installed applications that run as a service.

## System State data

All the files that belong to VSS writers with a usage type of BootableSystemState or SystemService. You require these files to perform an offline recovery.

## User data

Data that users generate, typically for the purposes of a business function. For example, a Microsoft Word document or an Excel spreadsheet. Windows BMR does not back up or recover user data unless the data resides on a critical volume. The simplest way to back up all user data is to specify the keyword All in the backup save set of the client resource. You can recover user data online at any time (on demand) or after a Windows BMR recovery operation.

## WinPE

A bootable stripped-down version of the Windows operating system. The NetWorker Windows BMR image contains a customized WinPE with NetWorker binaries and a wizard to control the offline recovery process. WinPE does not support writers, except for the ASR writer. Therefore, VSS writers are not available with a NetWorker Windows BMR.

# Overview of Windows Bare Metal Recovery (BMR)

NetWorker Windows BMR is an automated recovery solution that uses the Windows ASR writer and other Microsoft VSS writers to identify critical volumes and perform a full recovery on a target host.

NetWorker Windows BMR supports file system backup and recovery. NetWorker Module for Microsoft (NMM) supports application data backup and recovery. Additional backup and recovery procedures are required to backup and restore application data. The NMM documentation provides specific instructions on how to backup and recover applications.

NetWorker uses a special save set called the DISASTER\_RECOVERY:\ save set to backup all of the data required to perform a Windows BMR recovery. NetWorker performs the Windows BMR backup while the Windows operating system is inactive. You can recover an offline Windows BMR backup without first reinstalling the Windows operating system. This prevents problems that can occur when you restore operating system files to a running version of Windows.

To support a NetWorker Windows BMR recovery, you must download the Windows BMR image from the <http://support.emc.com> website. This download enables you to create a bootable Windows BMR ISO that contains NetWorker binaries and a wizard, which controls the recovery process.

---

**Note**

The *EMC NetWorker Software Compatibility Guide* provides more information about operating systems support for Windows BMR.

Components of the DISASTER\_RECOVERY:\ save set

---

The DISASTER\_RECOVERY:\ save set contains a group of component save sets that are required to perform a Windows BMR recovery. A full backup of the DISASTER\_RECOVERY:\ save set contains the following components:

- All critical volumes
- WINDOWS ROLES AND FEATURES
- System Reserved partition
- UEFI partition (if available)

NetWorker supports full and incremental backup levels of the DISASTER\_RECOVERY:\ save set. When the Windows BMR recovery operation recovers data from an incremental backup, the recovery operation will recover all incremental backups from the last full backup.

The first time NetWorker performs a backup of the DISASTER\_RECOVERY:\ save set, NetWorker will perform a level Full backup, regardless of the level defined for the backup.

When you configure an level Incremental backup of the DISASTER\_RECOVERY:\ save set, NetWorker backs up some components of the DISASTER\_RECOVERY:\ save set at a level Full.

The following table summarizes the backup level of each save set component of the DISASTER\_RECOVERY:\ save set, when you perform an incremental backup:

**Table 108** DISASTER\_RECOVERY:\ components in an incremental backup

| Save set                   | Backup level |
|----------------------------|--------------|
| Critical volumes           | Incremental  |
| WINDOWS ROLES AND FEATURES | Full         |
| UEFI partitions            | Full         |
| System reserved partition  | Full         |

During an incremental backup, the backup operation checks both the modification time and the archive bit to determine if a file needs to be backed up. The backup operation will ignore the archive bit when you set the environment variable on the client host. As a result, NetWorker backs up all of the files with every incremental backup.

Use the environment variable nsr\_avoid\_archive with caution. If you use the environment variable nsr\_avoid\_archive, test your BMR backup image to ensure that you can recover your Windows system state correctly. The topic Performing a BMR recovery to a physical computer provides more information on validating your BMR backup image.

A Windows BMR recovery requires a successful backup of each component save set in the DISASTER RECOVERY:\ save set. If one component of the save set fails, then the backup operation fails. For a scheduled backup, NetWorker retries the DISASTER\_RECOVERY:\ backup based on the value defined in the Client retries attribute for the Group resource.

---

**Note**

In NMC Administration, the **Log** tab of the **Monitoring** window or the **Save Set** tab of the **Media** window displays each component save set of a DISASTER\_RECOVERY:\ backup.

---

## Critical volumes

This topic describes critical volumes and the associated management tools.

NetWorker considers a volume as critical when it contains files for an installed Windows service. NetWorker also considers the following volumes as critical and will include the volumes in a DISASTER\_RECOVERY:\ backup:

- A non-critical volume that has a critical volume mounted on it, or a non-critical volume that serves as a parent to a critical volume.
  - All volumes on a dynamic disk when one of the volumes critical. If one disk in a dynamic disk pack is critical, then NetWorker must treat all disks in that pack as critical. This can substantially increase the number of disks that NetWorker includes in the BMR backup. EMC recommends that you do not install services on a dynamic disk.
- 

**Note**

By default, the Windows 2012 System Writer does not report Win32 Service Files as a part of systems components. As a result, the volumes that contain Win32 Service Files are not considered critical and the DISASTER\_RECOVERY:\ save set will not include a volume that contains files for an installed service. To configure the Windows 2012 server to report Win32 Service Files as a part of system components, set the ReportWin32ServicesNonSystemState registry sub key to 0. Microsoft KB article 2792088 provides more information.

---

A Windows BMR backup does not back up the following files on a critical volume:

- Files listed in the FilesNotToBackup registry key
- Files excluded by system writers
- Files that an application VSS writer backs up. For example, Exchange databases. Use NetWorker Module for Microsoft Applications (NMM) to backup these files.

### **Excluded critical volumes during a Windows BMR backup**

A NetWorker Windows BMR backup excludes critical volumes based on the operating system, disk types, configuration and installation of your computer.

Install applications with third-party services on the system disk, or a disk that already has other services installed. To identify the disks that contain third-party services, use the utility, list writers detailed command.

For Windows Server 2008 and 2008 R2, set the ExcludedBinaryPaths registry key to exclude third-party services from the System Writer. This prevents the disk where the service is installed from being classified as critical. The Microsoft support document *System state backup error in Windows Server 2008, in Windows Vista, in Windows 7 and in Windows Server 2008 R2: "Enumeration of the files failed"*, available at <http://support.microsoft.com/kb/980794>, describes the use of this registry key.

NetWorker excludes a volume from a backup when one of the following Windows application service is installed on the host:

- Storage Spaces volume
- Cluster volume

- Cluster Shared Volume

**NOTICE**

To ensure that you can recover all required files, perform a file system backup of any excluded disk.

---

### Displaying a list of the critical volumes

To view a list of the critical volumes for a NetWorker client, type the NetWorker command **save -o vss:LCV=yes** from the command line on the client host.

For example:

```
NetWorker_install_path\bin>save -o VSS:LCV=yes
```

Output similar to the following appears:

```
The following volumes are determined as critical by the system
state writers:
  C:\ (disk num 0)
  i:\mount\ (disk num 7)
  The following volumes are critical because they are parents for
one or more mounted critical volumes:
    i:\ (disk num 2)
    The following volumes are critical because they are in the
same dynamic disk pack with one or more critical volumes:
      H:\ (disk num 4,5)
      i:\ (disk num 2)
```

## WINDOWS ROLES AND FEATURES save set

The WINDOWS ROLES AND FEATURES save set was introduced in NetWorker 8.1 and replaces the VSS SYSTEM BOOT, VSS SYSTEM FILESET and VSS SYSTEM SERVICES save sets. The DISASTER\_RECOVERY:\ save set contains the WINDOWS ROLES AND FEATURES save set as a component save set.

This save set contains:

- Data associated with the roles and features that are installed on the Windows server.
- Metadata that represents the volume data which the ALL or DISASTER\_RECOVERY:\ save set backs up.

Before you backup the WINDOWS ROLES AND FEATURES save set, consider the following:

- Block Based Backups (BBB) do not support the WINDOWS ROLES AND FEATURES save set.
- You cannot restore the WINDOWS ROLES AND FEATURES save set at the same time as data from a file system backup. If you need to recover data from both the WINDOWS ROLES AND FEATURES backup and a file system backup, restore the file system data first, and then restore the WINDOWS ROLES AND FEATURES data.
- You can perform an online recovery of the WINDOWS ROLES AND FEATURES save set to recover the Active Directory, DFSR, or Windows Server Failover Cluster services. The topic *Online recovery of Active Directory, DFSR, or Cluster services* provides more information.
- If you cancel a deduplication recovery, the state of the recovered data is not reliable and may contain corrupted data. To ensure the recovery is correct, restart the deduplication recovery process.
- The backup operation will only confirm that the VSS System Writer exists on the target host. If the backup operation does not detect the writer, the backup of the

**DISASTER RECOVERY:\** or ALL save set fails. The backup operation does not track and report any other missing VSS writers.

- You can perform a component level granular restore of the WINDOWS ROLES AND FEATURES save set with a command line recover or the NetWorker User application. For example, you can recover the system state and replication folders separately. You cannot use the NMC Recovery UI to perform a component level restore.
- Do not restore the Windows Roles and Features system state multiple times in succession without rebooting the computer as required. If you do not reboot the computer, you can put the system in an unreliable operational state.

#### Note

The NetWorker 8.2 and later client can only recover WINDOWS ROLES AND FEATURES save sets. If you attempt to recover a VSS System State save set that was created with a NetWorker 8.0 SP1 client or earlier, then the Windows host will not function correctly. To recover VSS system state save sets created with a NetWorker 8.0 SP1 or earlier backup, use the NetWorker 8.0 SP1 or earlier client to create a backup. EMC recommends that you restore the WINDOWS ROLES AND FEATURES saveset from a NetWorker 8.1 or later backup.

## UEFI Partition Support

NetWorker supports a backup and recovery of unmounted partitions on hosts that use a supported . The *EMC NetWorker Software Compatibility Guide* provides more information about support operating systems.

The topic *Performing a Windows BMR recovery to a physical computer* describes how to perform a Windows BMR of a computer that has UEFI partitions.

The following list summarizes the properties of a UEFI partition backup:

- NetWorker can backup an unmounted partition.
- NetWorker uses the following path pattern to backup the UEFI partitions:  
\\<root>\Device\HarddiskVolume#  
where # is the number of the volume.
- The DISASTER\_RECOVERY \: save set contains a backup of the UEFI partitions.
- NetWorker always performs a level Full backup of UEFI partitions, regardless of the backup level of the DISASTER\_RECOVERY save set.
- NetWorker does not index the UEFI partitions or make the UEFI partitions available for online recoveries.

After a successful BMR restore, a host that uses UEFI might fail to boot. This can occur when the UEFI boot manager does not have a valid Boot Order entry, for example, when you delete the Boot Order entry or restore the Windows BMR backup to different hardware. In these situations, the operating system recreates the Boot Order entry during a reboot operation but may not use the same path.

To resolve this issue, load Boot Manager and select **Boot** from the **File** menu to correct the Boot Order entry.

## Windows Server 2012 Cluster Shared Volumes (CSV)

NetWorker does not support Windows Server 2012 Cluster Shared Volumes () as a critical volume. If a CSV disk is marked as a NetWorker critical disk, then the Windows BMR backup reports a warning, and continues to perform the backup operation as if the CSV is

not on the critical list. NetWorker does not backup the CSV because a CSV cannot reside in the same shadow copy set with a local volumes.

Applications such as SQL Server and Hyper-V in a Windows Continuous Availability scenario using CSV are not supported.

The *EMC NetWorker Cluster Integration Guide* provides more details.

## Windows Server 2012 Storage Spaces

NetWorker Windows BMR does not support the backup and recovery of critical System State data located on virtual disks. A NetWorker BMR backup skips all critical volume data located on Storage Spaces and does not add the volume to the BMR critical volume list. A BMR recovery cannot recover critical volume data on Storage Spaces. As long as the Storage Pool disks that compose a Storage Spaces virtual disk are not damaged, a recovery operation to the original computer will mount the Storage Pool virtual disks after the critical volume recovery operation completes.

**NOTICE**

EMC recommends that you detach the physical disks that Storage Spaces use when you recover critical volumes, and then reattach the physical disks after recovery. A Window BMR recovery operation can overwrite data on attached Storage Spaces disks.

---

The topic *Windows Storage Pools considerations* describes how to perform a Windows BMR recovery of Storage Spaces to a new computer.

**NOTICE**

---

To backup and recover data on virtual hard disks and volumes created by Storage Spaces, use NetWorker file system backup and recovery operations.

A Windows BMR backup of a Windows 2012 host creates a new file named `OSSR_sysinfo.xml`. The file is located at `[root]\EMC_NetWorker\nsr\tmp`. This file captures pertinent information about the configuration of the backed up host. For example:

- Host information (name, boot drive, BIOS or EFI)
- NIC cards and their parameters
- Disk information
- Storage Spaces information

The purpose of this file is to support the manual recreation of the Storage Spaces configuration following a BMR recovery.

## Synthetic full backups

A synthetic full backup uses the most recent full and incremental backups to create a full backup without transferring any data from the client. NetWorker performs all of the work to synthesize a full backup on the NetWorker server. A synthetic full backup gives you the benefits of a full backup, such as a faster restore, without having to perform a full backup.

The topic *Synthetic full backups* describes the synthetic full backup feature.

When a client backup includes the `DISASTER_RECOVERY:\` save set, NetWorker will always backup volumes identified as critical, at a level full. NetWorker will not create a synthetic full backup for critical volumes. The `DISASTER_RECOVERY:\` save set is included during full backups when either the All or `DISASTER_RECOVERY:\` save set is specified in the NetWorker client resource.

### Example: Synthetic full backups with save set All

The Save set attribute of the client resource contains the All save set and the backup schedule includes a synthetic full backup on Sundays. The NetWorker client host has four volumes: two are critical, and two are non-critical.

- C:\ and E:\ are critical volumes.
- F:\ and G:\ are non-critical volumes.

On Sundays, NetWorker performs a backup of the following save sets:

- C:\ — At a true level full backup level.
- E:\ — At a true level full backup level.
- F:\ — At a synthetic full backup level.
- G:\ — At a synthetic full backup level.
- DISASTER\_RECOVERY:\ — At a true level full backup level.

### Example: Synthetic full backups with file system save sets

The Save set attribute of the client resource contains a list of all volumes and the backup schedule includes a synthetic full backup on Sundays. The Save set attribute does not contain the DISASTER\_RECOVERY:\ save set. The NetWorker client host has four volumes: two are critical, and two are non-critical.

- C:\ and E:\ are critical volumes.
- F:\ and G:\ are non-critical volumes.

On Sundays, NetWorker performs a backup of the following save sets:

- C:\ — At a synthetic full backup level.
- E:\ — At a synthetic full backup level.
- F:\ — At a synthetic full backup level.
- G:\ — At a synthetic full backup level.

## Online recovery of Active Directory, DFSR, or Cluster services

The DISASTER RECOVERY:\ save set includes the WINDOWS ROLES AND FEATURES component save set, which you can recover the backup in an online recovery operation, to a host that uses the same Windows operating system instance. NetWorker 8.2 and higher support the online recovery of the following Windows services, which the WINDOWS ROLES AND FEATURES component contains:

### Active Directory

SolVe Desktop provides procedures that describe how to recover this service.

### Distributed File System Replication (DFSR)

The topic, Backing Up and Restoring a Microsoft DFS, provides more information.

### Cluster

SolVe Desktop provides procedures that describe how to recover this service.

NetWorker does not support the online recovery of any other Windows service that the WINDOWS ROLES AND FEATURES save set contains. Unsupported online recovery of WINDOWS ROLES AND FEATURES components will result in an inconsistent state of the Windows server.

**NOTICE**

When you perform an online recovery, you cannot mark the WINDOWS\_ROLES\_AND\_FEATURES save set and use the Required Volumes option. To determine the volume that contains the WINDOWS\_ROLES\_AND\_FEATURES save set that you want to restore, mark the DISASTER RECOVERY save set, then use the Required Volumes option. After you determine the required volumes, unmark the DISASTER RECOVERY :\ save set and mark the WINDOWS\_ROLES\_AND\_FEATURES save set.

---

## Windows BMR Planning

This section provides guidelines on how to plan your Windows BMR backups.

### Hardware Requirements for Windows BMR backup and restore

The BMR recovery process restores the operating system that was installed on the source host. If you perform a BMR recovery to a different host with different hardware, after the recovery operation and reboot completes, Windows will prompt you to install the required drivers.

Before you perform a BMR recovery to a different host, ensure that you meet the following requirements:

- The source and target hosts use the same operating system architecture and processor architecture.
- The hardware on the target host is operational.
- The target host has a minimum of 512 MB of RAM.
- The capacity of the startup hard disk on the target host is larger or the same size as the startup hard disk on the source host. If the disk on the target host is smaller by a single byte, the BMR recovery operation will fail.
- The number of disks on the target host is greater than or equal to the number of disks there were on the source host. The disk LUN numbering on the target host must match the disk LUN numbering on the source host.
- The RAID configuration on the target computer cannot interfere with the disk order of the hard disks.
- The disk or RAID drivers used on the source system are compatible with the disk or RAID controllers in the target system. The recovery process restores the backup to the same logical disk number that was used by the source host. You cannot restore the operating system to another hard disk.
- Windows BMR supports IDE, SATA, or SCSI hard disks. You can make the backup on one kind of hard disk and recover on another kind of hard disk. For example, SAS to SATA is supported.
- The target system can access the Windows BMR image as a bootable CD volume or from a network boot location.

After the Windows BMR recovery completes and the host reboot occurs, you must install NIC drivers that match the NIC in the target computer. All NIC or storage device drivers must not require a reboot to complete the driver installation process. If the drivers require a reboot, then the BMR recovery process restarts and will prompt you to install the drivers again.

## Save set configuration by host type

This section describes the attributes of save sets used by Windows BMR. This information helps you select the correct save set configuration for your computer and operating system.

The following table lists the save sets to back up, depending on the Windows host to be protected.

**Table 109** Save set configuration for a specific host

| To back up this host                                                                                                                                   | Specify these save sets in the client resource Save Set attribute                                                                                                                                                                  | Considerations                                                                                                                                                                                                                                                                                                                                                                                    |
|--------------------------------------------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| A host or file server that is not a Microsoft Application server                                                                                       | <ul style="list-style-type: none"> <li>Specify the save set All in the NetWorker client resource.</li> <li>By default, the save set All includes the DISASTER RECOVERY:\ save set and all of the local physical drives.</li> </ul> | <ul style="list-style-type: none"> <li>WINDOWS ROLES AND FEATURES must be backed up.</li> <li>WINDOWS ROLES AND FEATURES save sets are recovered in a Windows BMR operation and are also available for online recovery. WINDOWS ROLES AND FEATURES save sets should only be recovered online as part of an Active Directory, DFSR, or Windows Server Failover Cluster online recovery.</li> </ul> |
| A host that is a Microsoft Application server. For example, a Microsoft Exchange Server, Microsoft SQL Server, Hyper-V, or Microsoft SharePoint Server | <ul style="list-style-type: none"> <li>Specify the ALL save set in the Save set attribute in the NetWorker client resource.</li> <li>Use NMM to back up the application databases. The NMM provides details.</li> </ul>            | <ul style="list-style-type: none"> <li>Use the Windows BMR Wizard to recover the data contained in the DISASTER RECOVERY:\ save set.</li> <li>Use NMM to recover the application databases.</li> </ul>                                                                                                                                                                                            |

## Best Practices for Windows BMR

The following sections outline best practices for Windows BMR.

### Perform regular backups

Perform a full backup that contains the DISASTER\_RECOVERY:\ save set regularly and after any you install, remove or update any system components. For example, when you add, change, or remove Windows roles and features, or install Windows updates and service packs.

NetWorker will automatically back up the DISASTER\_RECOVERY:\ save set when you specify the ALL save set in the Save Set attribute of the NetWorker client resource.

## Capture disk configuration changes for Windows BMR

The NetWorker BMR recovery operation uses the Microsoft ASR writer to reconstruct a disk configuration. The ASR writer is sensitive to the disk numbers and disk configuration of the original host. NetWorker saves this disk information during a Windows BMR backup and uses the disk configuration information to perform the recovery. After you reconfigure any disk on a host, reboot the host and then perform a Windows BMR backup to ensure that NetWorker captures the new disk configuration. Examples of a disk reconfiguration include the addition or removal of a disk or partition.

## Mixing critical and non-critical volumes on a physical disk

Windows allows you to partition a physical disk into multiple volumes. These volumes can be either critical or non-critical, depending on the type of data that they contain. During a Windows BMR recovery operation, the ASR writer can re-create and format a partition, including non-critical partitions. If the ASR writer formats a non-critical partition, you must use an online recovery to data on the non-critical partitions. The topic, *Recovering file system data*, describes how to perform an online recovery.

### NOTICE

Do not mix critical and non-critical volumes on the same physical disk.

---

## Considerations for NetWorker user defined directives

Use user defined directives, such as *nsr.dir*, with caution. When you use directives in directories where system state and installed services data resides, the backup will create an incomplete BMR backup image and potentially render your BMR backup image unusable. If you create user defined directives, test your BMR backup image to ensure that you can successfully perform a BMR Recovery. The topic, *Performing a Windows BMR recovery to a physical computer*, provides more information about testing your BMR backup image.

## Critical volume recommendations

Use the following practices to minimize the size of Windows BMR backups.

- Do not store non-critical data, such as MPEG files, on critical volumes.
- Consolidate critical volumes. For example, install services on the same disk.
- Do not mount critical volumes on a non-critical volume.

## Windows BMR limitations and considerations

Review the following Windows BMR limitations and special considerations before you perform Windows BMR backup, clone and recovery operations.

### Disk configuration limitations

This section describes disk configuration limitations in Windows BMR.

#### Dynamic disks

A BMR recovery does not bring dynamic disk volumes online. After the BMR recovery completes, use Windows Disk Manager to bring the dynamic disks back online.

#### NTFS and ReFS

Only NTFS and ReFS file systems are recognized as critical volumes

Although the backup of the DISASTER\_RECOVERY:\ save set fails, NetWorker will backup, the contents of the partition and the data is available for an online recovery only.

To ensure a successful backup of the DISASTER\_RECOVERY:\ save set, install all services or application on an NTFS or ReFS volume.

#### Critical volumes

Windows BMR only supports critical volumes on NTFS and ReFS partitions. This is a Microsoft ASR limitation. If a critical volume is on a partition other than NTFS or ReFS, the backup of the DISASTER\_RECOVERY:\ save set fails. A message similar to the following appears in the savegrp.log file:

```
Disaster Recovery: critical volume volumename identified for disaster recovery backup has a non-NTFS file system, filesystemname. Backups of non-NTFS critical volumes are not supported.
```

#### Note

Windows BMR does not support FAT and FAT32 file systems as critical volumes.

## HP ProLiant system considerations

You cannot recover from a Windows BMR backup on an HP ProLiant system when the HP i Provisioning Tool (IPT) 1.4 or 1.5 was used to configure an entire disk as a critical volume, such as the system partition.

To resolve this issue, shrink the logical volume before you perform the Windows BMR restore. The HP website contains a customer advisory that describes the issue and the impact to Windows Bare Metal Recovery with Windows Server Backup. This advisory and the resolution also applies to NetWorker Windows BMR critical volumes.

#### Note

EMC recommends that you test your BMR solution before a disaster recovery is required.

## Optimized deduplication backup considerations

Review this section before you configure backups that use optimized deduplication.

- You can recover a complete volume backup recovery to the original volume only if the backup was performed at a level Full.
- You cannot recover specific files from a level FULL or INCREMENTAL save set.
- You cannot perform a full volume recovery of a non-full level save set.
- You cannot recover data from an optimized and unoptimized deduplication backup when VSS is disabled. The backups that NetWorker created are corrupt.
- You cannot cancel the recovery of an optimized deduplication backup to a deduplication volume. If the recovery process is interrupted or fails, the destination volume becomes unusable. You must repeat the recovery process and the recovery operation must complete successfully to prevent volume corruption.
- If the optimized deduplication recovery cannot successfully complete, you can perform a selected files restore of directories from the optimized deduplication backup. This restores the directories' files to a rehydrated state, but will take significantly more time.

## Save set considerations

This topic describes limitations and considerations that relate to save sets.

### **Checkpoint restart backup for Windows DISASTER\_RECOVERY:\ save set is not supported**

The NetWorker software does not support a checkpoint restart backup for the Windows DISASTER\_RECOVERY:\ save set. When you enable the Checkpoint restart option for a client resource that you configure to back up the DISASTER\_RECOVERY:\ save set, the backup will fail.

### **Including DISASTER\_RECOVERY:\ in multiple save sets**

When you use specify multiple save sets with the save command, you must use the -N option to specify the symbolic name of DISASTER\_RECOVERY:\ save set, and specify the DISASTER\_RECOVERY:\ as the last save set in the save set list.

For example:

```
save.exe -s server -N "DISASTER_RECOVERY:\\\" save_set1 save_set2 ...  
"DISASTER_RECOVERY:\\\"
```

where:

save\_set1 or save\_set2 are unique save set names, such as a drive letter (f:\) or mount point (n:\mountpoint).

### **Monitoring save operations**

When you monitor Windows BMR save operations, for example, by using the NetWorker Administration > Monitoring > Sessions window, you might notice that the number of save sessions differ from the number of save sets that appear in the Save set attribute of the client resource. This is because NetWorker optimizes Windows BMR backups to generate the correct number of Windows BMR backup sessions and save sets.

## Cloning considerations

To clone a Windows BMR backup, ensure that you clone all of the critical volumes, DISASTER\_RECOVERY:\, and WINDOWS ROLES AND FEATURES save sets that were created during the backup operation. While you can clone individual save sets, you cannot perform a successful BMR recovery unless you recover each save set that the backup operation created.

To ensure that you clone all of the BMR save sets, review the following information before you start a clone operation:

- When you use the automatic clone, you enable the Clone attribute on the group resource that contains the BMR client. The automatic clone operation will clone all of the required save sets after the scheduled backup operation completes.

---

### **Note**

Synchronize the NetWorker server and client host clocks before the backup operation to ensure that all of the save sets are cloned.

- When you use the nsrclone command to perform a manual clone, ensure that you include the *ssid/cloneid* for each save set. Use the *mminfo* or *nsrinfo -v* command to report all save set back ups that occurred for the Windows client during the save session. The *Command Reference Guide* provides detailed information about using the *mminfo* and *nsrinfo* commands.
- When you use the schedule clone function, do not filter on other attributes such as save set name. Filter only by client name. When you enable automatic cloning for a backup group that contains the DISASTER\_RECOVERY:\ save set, synchronize the

clocks on the NetWorker server and client host clocks across the network. to ensure that NetWorker clones all of the save sets.

## Security considerations

This section describes security issues related to Windows BMR planning.

### **NetWorker Strong Authentication and Windows BMR recoveries**

When you recover a Windows client that uses NetWorker strong authentication (nsrauth) to communicate with other NetWorker hosts, communications with the NetWorker server may fail after a Windows BMR recovery. When you perform a Windows BMR recovery for a host that uses nsrauth authentication only, the Windows PE image does not have the nsrauth credentials file that the original client used and the NetWorker server will refuse to allow the recovery operation to complete.

To resolve this issue, before you perform the BMR recovery perform one of the following tasks:

- Delete the NSR Peer Information resource for the NetWorker client from the NSRLA database on the NetWorker server. This will cause the NetWorker server to create a new NSR Peer Information resource for the client.

#### **Note**

After the recovery operation and the client reboot completes, the client will attempt to use the original credentials to authorize communication with the NetWorker server, and the server will refuse communications. To resolve this issue, delete the NSR Peer Information resource for the Windows client from the NSRLA database on the Windows host. Deleting the NSR Peer Information resource in the *EMC NetWorker Security Configuration Guide* provides more information.

- Modify the authentication method that the NetWorker server uses to communicate with the Windows host, to ensure that communication attempts use oldauth. *EMC NetWorker Security Configuration Guide* provides more information.

#### **Note**

After the recovery operation and the client reboot completes, modify the authentication method that the NetWorker server uses to communication with the Windows host back to the original value.

## Server role considerations

This section describes considerations for Windows Server Roles in Windows BMR.

### **Protecting Windows server roles**

Several server role components of Windows host store the data in a database. Examples of Windows server roles with databases include:

- Active Directory Rights Management Services (ADRMS)
- Windows System Resource Manager (WSRM)
- Universal Description, Discovery, and Integrations (UDDI) Services
- Windows Server Update Services (WSUS)

When you install the Windows server role on a host, the installation process prompts you to store data on either an existing SQL Server installation or in a Windows Internal Database (WID).

NetWorker uses the VSS SQL Server writer to back up the role databases stored in WID but does not protect role databases, which the server role component stores in a SQL

Server. Use NMM or a third-party SQL backup product to backup and recovery the roles databases.

#### **Backup and recovery workflows for server roles that use WID**

These are the backup and recovery workflows are as follows:

- Perform a NetWorker Windows BMR backup, which includes all of the SQL writer components for WID. If required, backup user data on the client.
- Perform a NetWorker Windows BMR recovery operation, which recovers all of the WID components.

After the NetWorker Windows BMR system reboot, the WID service is available and Windows server roles have access to their databases.

Saving and recovering SQL Server components with Windows BMR and NMM:

1. Perform a NetWorker Windows BMR backup. If required, backup user data on the SQL client.
2. Use NMM or a third-party backup application to back up the SQL Server application.
3. Perform a NetWorker Windows BMR recovery operation.  
After the recovery and reboot operations complete, you cannot start the SQL Server service and any server roles that store data in SQL databases outside WID will not work.
4. For non clustered SQL servers only, ensure that the SQL group is offline.
5. Run the following **setup.exe** command from a command prompt with elevated privileges, to rebuild the SQL Server:

```
C:\> setup /QUIET /ACTION=REBUILDDATABASE /
INSTANCENAME=Instance_name /SQLSYSADMINACCOUNTS=domain_name
\administrator
```

#### **Note**

The SQL Server installation media contains the **setup** tool.

6. Bring the SQL sever services online.
7. Use NMM or a third-party backup application to recover the SQL system databases (master, model, msdb).
8. Use NMM or a third-party backup application to recover the role databases.
9. Restart the services that require the role databases that you recovered.

#### **NOTICE**

The *NetWorker Module for Microsoft Applications Application Guide* provides more information about using NMM to recover SQL databases.

## Microsoft server application considerations

Use both the NMM and the NetWorker software to protect Microsoft server applications, such as Microsoft Exchange Server, Microsoft SQL Server, Hyper-V, and Microsoft SharePoint. The NMM software protects the application data, such as databases and log files and the NetWorker client software protects the user data and critical disks on the host, for the purposes of Windows BMR.

Below is a high level overview of NetWorker and NMM backup and recovery workflow for Microsoft server applications:

1. Use NetWorker to back up critical and non-critical disks as part of a regular file system backup.
2. Use NMM to back up application data, such as Microsoft SQL Server.
3. Use NetWorker to perform a Windows BMR backup of the critical volumes on the host.
4. Use the Windows BMR boot image to perform a BMR recovery.
5. Use the NetWorker User application to recover any non-critical disks.
6. Use NMM to recover the application data.

The NetWorker Module documentation provides more information about recovering application data.

## Online recovery of Windows services considerations

This section describes limitations and considerations related to Windows services.

### Active Directory considerations

A Windows BMR recovery of a Domain Controller is non-authoritative by default. If you need to perform an authoritative recovery, then you must boot into DSRM mode directly from the Windows BMR wizard. The topic, *Performing post-recovery tasks for Active Directory services*, provides more information.

### DFSR considerations

DFSR namespaces are junction mount points. The DISASTER \_RECOVERY:\ and ALL save sets do not backup DFSR namespaces, even if the DFSR shares reside on a critical volume. To backup DFSR Shares, either use the new save set ALL-DFSR or provide the full DFSR Share path as the save set name. The ALL-DFSR save set applies to all supported platforms. Unlike the ALL save set, which skips the DFSR namespace because it is a junction point, the ALL-DFSR save set will back up every namespace, along with the associated replication folders.

The topic, *Recovering Windows volume mount points*, provides more information about recovering volume mount points.

### MSCS considerations

Review these considerations before you perform a Windows BMR recovery on a clustered host.

- Before you start the Windows BMR recovery operation, ensure that you detach the shared disks. After the Windows BMR recovery operation and the reboot completes, attach the shared disks before you perform the online recovery.
- After an authoritative restore completes, the recovery operation does not bring the cluster services online on the remote nodes. You must bring the services online manually.

## Windows Storage Pools considerations

When a system failure occurs which damages Storage Pools, perform the following steps as recommended by Microsoft to perform a BMR recovery to a new host. In the case of a complete system failure, a Storage Pool may not exist on the target host. There can only be physical disks. Some of these disks are required to create Storage Pools.

Before beginning Windows BMR wizard, physically remove from the target recovery computer any physical disks reserved for storage pools. This manual step is required because the Windows BMR wizard does not have any option to exclude the disks.

To recover Storage Spaces to a new host, perform the following steps:

1. Boot the host with the Windows BMR image.

2. Recover only the critical volumes.
3. Reboot the host.
4. Attach physical disks that are reserved for Storage Pools.
5. Use Windows Server Manager or Powershell Cmdlets to configure the Storage Pools.
6. Perform a volume or file recovery of the Storage Spaces volumes.
7. Perform a volume or file recovery of other volumes on physical disks.

## WinPE considerations for SAN boot devices

When you recover to a host that uses a SAN boot device, the WinPE environment requires that you temporarily disable all but one path to the boot device. After the BMR recovery and reboot completes you can re-enable the remaining paths.

## VMware network interface card driver limitations

The Windows BMR image does not contain a driver for any of the VMware VMXNET, VMXNET3, or the VMware Paravirtual SCSI NIC models. The Windows BMR image does contain a driver for the e1000 NIC. When you perform a Windows BMR recovery, ensure that the VM has at least one configured e1000 NIC, or add custom NIC drivers when you run the NetWorker BMR wizard.

The VMware Tools installation media in the \Program Files\VMware\VMware Tools\Drivers folder on the system drive of the VM contains the VMware NIC drivers.

## BCD partition limitations

NetWorker requires that the BCD partitions are online during a Windows BMR backup. If a BCD partition is offline during a Windows BMR backup, the backup fails with an messages similar to the following:

```
save: Unable to get volume information of file system. The device is
not ready. (Win32 error 0x15) with the volume offline
```

# Performing a Windows BMR backup

You can run Windows BMR backups on a scheduled basis (full backups only) or manually (on demand). This section describes how to plan and set up Windows BMR backups.

## Including Windows BMR in scheduled backups

Although you can back up the DISASTER\_RECOVERY:\ save set separately, the easiest way to schedule Windows BMR backups is to specify the save set All. Specifying the save set All ensures that all System State data and user data can be recovered in the event of a disaster.

---

### Note

To backup Active Directory, DFSR or Cluster Services, ensure that you perform DISASTER\_RECOVERY:\ backup.

---

To set up a Windows Server 2008, Windows Server 2008 R2, Windows 7, Windows Server 2012, Windows 8, Windows Server 2012 R2, or Windows 8.1 client for scheduled Windows BMR backups, you can use either the NetWorker Client Configuration wizard or the NetWorker client properties window.

## Configuring Windows BMR backups by using the wizard

### Procedure

1. Use NMC to connect to the NetWorker server.
  2. In the **Configuration** view, expand the NetWorker server, right-click **Clients**, and then select **New Client Wizard**.
  3. On the **Specify the client name and type** window, specify the name of the host and select **Traditional NetWorker client**, then click **Next**.
  4. On the **Specify the Client Backup Options** window, select options as required, then click **Next**.
- 

### Note

Ensure that you do not select **Checkpoint enabled**.

5. On the **Select the Backup Application Type** window, select **Filesystem**, then click **Next**.
6. On the **Select Files to Back Up** page, leave the default selection, which includes the filesystem and Windows BMR backup. To perform a BMR backup only, expand the host and select only the **DISASTER\_RECOVERY:\** save set. Click **Next**.
7. Complete the wizard, as instructed.

## Configuring Windows BMR backups from the properties window

[Backing Up Data on page 59](#) provides more information about setting up a scheduled backup.

### Procedure

1. Use NMC to connect to the NetWorker server.
2. In the **Configuration** view, expand the NetWorker server, right-click **Clients**, and then select **New**.
3. In the **Name** attribute, specify the hostname for the client.
4. Optionally, type a comment in the **Comment** attribute.
5. Select values for **Browse Policy** and **Retention Policy**:
  - The browse policy determines how long NetWorker maintains the details of each individual backup file to enable a browsable recovery.
  - The retention policy determines how long NetWorker protects data and makes the data available for recovery, even though the browse policy has lapsed. Recovery might require rebuilding index entries for the backup.
6. In the **Save set** attribute of the client resource, type **All** to back up the filesystem and perform a Windows BMR backup. To perform a BMR backup only, type **DISASTER\_RECOVERY:\**.
7. In the **Group** attribute, select a backup group. Ensure that you do not select a snapshot group.
8. In the **Pool** attribute, select a pool that enables write operations to volumes in the NetWorker devices that you want to use. The pool that you select overrides any other pool that might be configured for the client or its save sets.
9. In the **Schedule** attribute, select a backup schedule. The schedule selected in this attribute overrides any other schedules that might be configured for the client or its save sets.

10. When you have completed the client configuration, click **OK**.
11. In the **NetWorker Administration** window, the configured client appears with a checkmark in the **Scheduled backup** column to indicate that scheduled backup is enabled.

## Including Windows BMR in manual backups

When you use the NetWorker User program to back up a host, to ensure the backup operation will backup all of the data on the host, select Computer in the Backup window.

If you only select the DISASTER\_RECOVERY:\ save set, then the NetWorker User program automatically selects the critical volumes and WINDOWS ROLES AND FEATURES save sets.

### Note

When you use the NetWorker User program or the save command to perform a manual backup, NetWorker performs the backup operation as a single backup stream. To multi-stream the backup operation, run a scheduled group backup.

[Backing Up Data on page 59](#) provides more information about manual backups.

## Verifying a valid Windows BMR backup

After you perform a Windows BMR backup, verify that the backup exists. NetWorker creates one save set for each critical volume backed up by the DISASTER\_RECOVERY:\ save set.

You can verify that the backup exists by using the NMC console, the NetWorker User program, or the nsrinfo program.

### NOTICE

If any of the components of the Windows BMR backup fail, then NetWorker does not create a DISASTER\_RECOVERY:\ save set and you cannot perform an offline recovery. The backup process may backup the WINDOWS ROLES AND FEATURES save sets or critical volumes, which NetWorker makes available for an online recovery.

### Verifying that a valid backup exists by using the NMC console

#### Procedure

1. Use NMC to connect to the NetWorker server.
2. In the **NetWorker Administration** window, click **Media**.
3. In the left pane, click **Save Sets**.
4. On the right pane, on the **Query Save Set** tab, specify the search criteria such as the **NetWorker Client Name** and a date range for the **Save Time**.
5. Select the **Save Set List** tab in the right pane to generate and display a list of save sets that meet the search criteria.

## Verifying that a valid DISASTER\_RECOVERY:\ save set exists by using the NetWorker User Program

By default, the Recovery window displays the most recent backup. To verify an older backup select the View > Change Browse Time menu option and specify a different backup date and time.

### Procedure

1. Start the NetWorker User program by using the **winworkr** command with the **-s** option to connect to the NetWorker server to which the source client data is backed up:

```
winworkr -s server_name
```

If the **-s** option is not entered and there is only one server detected, that server is connected automatically. If there are no servers detected, or if there is more than one server available, the Change Server dialog box appears, enabling you to choose the server.

2. Click **Recover** to open the **Source Client** dialog box.
3. Select the source client whose DISASTER\_RECOVERY:\ save set, then click **OK**.
4. Select a destination client, then click **OK**.
5. In the **Recover** window, browse and locate the save set named DISASTER\_RECOVERY:\.

## Verifying that a valid DISASTER\_RECOVERY:\ save set exists by using the nsrinfo program

Perform the following steps from a command prompt to query the client file index of the Windows host to display information about the DISASTER\_RECOVERY save set.

Type the following command at the command prompt:

```
nsrinfo -v -s server_name -N "DISASTER_RECOVERY:\\\" client_name
```

where:

- **server\_name** is the name of the NetWorker server.
- **client\_name** is the name of the client that performed the Windows BMR backup.

## Performing a NetWorker Bare Metal Recovery wizard test

Before you need to perform a Windows BMR, test the wizard to ensure that you can complete a recovery and that you have the required drivers. This task is especially important for 64-bit hosts that might require additional drivers. For both 64-bit and 32-bit hosts, the wizard must use drivers that do not require a reboot.

### NOTICE

After you test the wizard, you can safely exit the wizard before completing the entire recovery process.

### Procedure

1. Follow the procedures in [Performing a Windows BMR recovery to physical or virtual computers on page 632](#).

Verify the following as you step through the BMR recovery wizard screens:

- If DNS is not available, that the host can resolve the NetWorker server name by some method, such as a local hosts file.

- You can see the network interface that is required to communicate with the NetWorker server. If you cannot see the network interface, use the wizard to load the required NIC driver.
  - You can see the critical and non-critical disks for the host that is to be recovered. If you cannot see all of the disks, use the wizard to load the required disk drivers.
2. Click **Exit** to safely exit the wizard.
  3. Exit the command window.
- The system automatically reboots.

## Performing a Windows BMR recovery to physical or virtual computers

This section describes how to use the NetWorker Windows BMR image to perform a Bare Metal Recovery on protected hosts and VMware virtual machines.

Before you perform a BMR recovery on a host, verify that the new host meets the [Hardware Requirements for Windows BMR backup and restore on page 620](#) and ensure that you complete the tasks listed in this section.

### Gathering configuration information required by a Windows BMR recovery

Before you start a Windows BMR recovery, ensure that you have the following configuration information:

- The driver software for NICs or disk devices, if you perform the Windows BMR to a host with hardware that differs from the source host.
- The network name and IP address of the target host.
- The network name and IP address of the NetWorker server.
- The network name and IP address of the NetWorker storage node, if the target host uses a storage node that is not the NetWorker server.
- The default gateway and the name of the DNS server. If a DNS server is not available, use a local hosts file to resolve host name of the NetWorker server and storage nodes to the appropriate IP address.
- The NetWorker media volumes that contain the backup save sets.

### Obtaining the Windows BMR image

To perform a Windows BMR recovery, you will use the Windows BMR image available from the EMC Online Support website. <http://support.emc.com> to create a bootable CD or deploy for a network boot operation. The BMR image contains the Windows PE operating system. WinPE is only available in English. EMC does not provide localized versions of the Windows BMR wizard. When you use the image to boot the Windows host, the recovery process starts the NetWorker BMR wizard, which guides you through the recovery process.

You can use the 32-bit Windows BMR image to recover an x86 operating system on an x86 or x64 computer. You can only use the 64-bit Windows BMR image to recover a 64-bit operating system on a 64-bit computer.

---

**Note**

A BMR recovery treats the AMD and Intel processors as equivalent if they follow the same architecture. For example, you can recover the operating system from the backup of AMD x64 computer to an Intel x64 computer.

---

Downloading the recovery boot image:

**Procedure**

1. On the EMC Online Support website, search for “NetWorker Wizard ISO” at EMC Online Support and narrow the search results by selecting items associated with the NetWorker 8.2 release.
  2. On the **NetWorker Software Downloads** page, locate the section labeled **NetWorker 8.2 - Build > xxx**, where **xxx** is the build number of the released version, and then select the appropriate link to download a Windows BMR ISO recovery file:
    - For target hosts that run a 32-bit version of Windows, select NW 8.2 Windows BMR Wizard x86 to download the file  
[NetWorker\\_8.2.0.XXX\\_Windows\\_BMR\\_Wizard\\_x86\\_WinPE\\_50.iso](#)
    - For target hosts that run a 64-bit version of Windows or hosts that use UEFI volumes, select NW 8.2 Windows BMR Wizard x64 to download the file  
[NetWorker\\_8.2.0.XXX\\_Windows\\_BMR\\_Wizard\\_x64\\_WinPE\\_50.iso](#) where **xxx** is the build number.
- 

**Note**

The Microsoft Windows(R) Preinstallation Environment (PE) software included with this computer or software can be used for boot, diagnostic, setup, restoration, installation, configuration, test, or disaster recovery purposes only. NOTE: THIS SOFTWARE CONTAINS A SECURITY FEATURE THAT WILL CAUSE YOUR COMPUTER SYSTEM TO REBOOT WITHOUT PRIOR NOTIFICATION AFTER 72 HOURS OF CONTINUOUS USE.

---

**Note**

FOR AUSTRALIA ONLY. References to “Limited Warranty” are references to the warranty provided by the manufacturer or installer. This warranty is given in addition to other rights and remedies you might have under law, including your rights and remedies in accordance with the statutory guarantees under the Australian Consumer Law. Our goods come with guarantees that cannot be excluded under the Australian Consumer Law. You are entitled to a replacement or refund for a major failure and compensation for any other reasonably foreseeable loss or damage. You are also entitled to have the goods repaired or replaced if the goods fail to be of acceptable quality and the failure does not amount to a major failure.

Goods presented for repair could be replaced by refurbished goods of the same type rather than being replaced. Refurbished parts could be used to repair the goods.

For further information regarding this warranty and to claim expenses in relation to the warranty (if applicable), please contact the manufacturer or installer; see the contact information provided in the system packaging.

---

## Creating a Windows BMR bootable image

Create a Windows BMR bootable CD or a network boot location from the Windows BMR ISO image, which you downloaded from <http://support.emc.com>.

### Creating a Windows BMR bootable CD

Use the ISO image to create a bootable CD, then configure the host to boot from a CD.

#### Procedure

1. Open your CD creation software and select an option to burn an ISO image.
2. Browse to the location of the downloaded NetWorker Windows BMR image and complete the steps required to create a bootable CD with the image.

### Enabling a protected host to boot from a CD

#### Procedure

1. Start the host and enter the BIOS setup program, typically by pressing **F2**.

**NOTICE**

If you are restoring a virtual host such as a VMware virtual machine, you can set up options such as the host boot location from within vSphere. The VMware documentation provides specific steps.

2. Select the boot options menu and ensure that the CD boot option is at the top of the list of locations from which to boot.
3. Save your changes and exit the BIOS program.

### Creating a Windows BMR recovery network boot location

Ensure that you meet the following requirements for using the network boot option.

- The NetWorker clients that you protect with a Windows BMR backup must have the ability to boot from the network with a Pre-Boot Execution Environment (PXE).
- Configure and make available a Deployment Services server.
- Add the NetWorker Windows BMR boot image to the Deployment Services server so that a client host on the network can boot from it.

**Note**

[http://technet.microsoft.com/en-us/library/cc771670\(WS.10\).aspx](http://technet.microsoft.com/en-us/library/cc771670(WS.10).aspx) describes how to configure Windows Deployment Services in Windows Server 2008.

### Enabling a host to boot from the network

Your host should obtain an IP address from your WDS server, then prompt you to perform a network boot. Typically, a network boot is activated by pressing the F12 key.

#### Procedure

1. Start the host and enter the BIOS setup program, typically by pressing **F2**.

**NOTICE**

If you are restoring a virtual host such as a VMware virtual machine, you can set up options such as the host boot location from within vSphere. The VMware documentation provides specific steps.

2. Select the BIOS options necessary so that the network boot option is enabled. The BIOS documentation provides more information.
3. Save your changes and exit the BIOS program.

## Performing a Windows BMR recovery to a physical computer

Perform the following steps to recover a BMR backup to a physical host. If the target host uses UEFI volumes, unmount the UEFI volumes before you perform the recovery operation.

Review the following information before you perform a recovery operation to a host that differs from the original:

- Ensure that the hardware configuration of the target host is similar to the original host.
- Ensure that the NetWorker server has a client resource for both the source host and the target host.
- Ensure that the Remote Access attribute of the source client resource contains the account *SYSTEM@target\_client*. This enables the recovery process to perform a directed recovery.
- Add `user=system,host=target_client` to the Users attribute of Application Administrators user group.
- Ensure that you have a writeable volume available for the Default pool. After the recover operation recovers all of the data, the wizard generates log files in a save set named Offline Restore Logs. The recovery operation performs a backup of the log files to a volume in the Default pool.
- Ensure that you enable the NetWorker server to accept manual save operations for the recovery wizard log file backup.

### Procedure

1. Boot the target host from the Windows BMR image. The NetWorker **Windows BMR wizard** appears.
2. On the **Welcome** screen, click **Next**.
3. If a DNS server is not available on the network, perform the following:
  - a. Exit the NetWorker **Windows BMR wizard** but do not reboot the host.  
The WinPE command line appears.
  - b. Edit the hosts file, for example, `X:\Windows\System32\Drivers\etc\hosts`, and add the IP address and hostname for the NetWorker server, the NetWorker storage node, and the Avamar deduplication node, if one is used.
  - c. Restart the wizard from the `X:\Program Files\EMC Networker\nsr\wizard` directory.  
For example: `X:\Program Files\EMC Networker\nsr\wizard>javaw -jar WinPEWizard.jar`

- d. When the wizard appears, click **Next**.
  4. On the **Select Network Interface** screen, select the NIC driver and then click **Next**.
    - If the driver list does not contain the driver for the NIC on the target host, select **Load Driver** and browse to the location that contains the required driver.
- NOTICE**
- The selected driver cannot require a reboot operation because the recovery process loads the WinPE environment in memory only and changes are not persistent after a reboot operation.
- 
5. On the **Configure Hostname and Network** screen, complete the fields :
    - a. In the **Hostname** field, type the hostname of the source host.
    - b. In the **DNS domain** field, type the name of the domain in which the host resides.  
If the host resides in a workgroup instead of a domain, you can leave this field blank.
    - c. In the **Configure desired IP Settings** field, choose the tab for the Network Protocol deployed on your network, either **IPv4** or **IPv6**.
    - d. In the **TCP/IP Address** settings section, select either **Obtain an IP address automatically (DHCP)** or **Use the following IP Address**.
      - If you choose **Use the following IP Address**, then type the IP address in the IP address field.  
If applicable, type the subnet mask in the **Subnet mask** field and the default gateway in **Default gateway** field.
    - e. In the **DNS Server** section, select either **Obtain DNS server address automatically** or **Use the following DNS server address**.
      - If you choose **Use the following DNS server address**, type the IP address of the DNS server in the **Preferred DNS server** field.
      - If applicable, type an alternate DNS server address in the **Alternate DNS server** field.
- NOTICE**
- You can ignore the DNS Server fields if you added the NetWorker server hostname and IP address to the `X:\Windows\System32\Drivers\etc\hosts` file.
- 
- f. Click **Next**.  
The **Available Disks** screen displays all detected local disks.
  6. If the Windows BMR wizard fails to detect a disk, perform the following steps:
    - a. Select **Load Driver**.
    - b. Browse to the location that contains the disk driver and load the required disk driver.
    - c. Select **Refresh** to update the list of detected disks.
    - d. Click **Next**.
  7. On the **Select NetWorker Server** screen, complete the fields:
    - a. In the **Server** field, specify the NetWorker server that performed the backup:

- Select the NetWorker server from the server list. Click **Search** to update the list of NetWorker servers. The Search function locates only those NetWorker servers on the local subnet.
  - Type the fully-qualified domain name (FQDN).
- b. In the **Client** field, ensure that the client name matches the client resource name on the NetWorker server.
- For example, if the client resource on the NetWorker server uses a FQDN, then specify the FQDN of the client in the **Client** field.
- NetWorker automatically populates this field with the values that you specified in the **Hostname** and **DNS Domain** fields on the **Configure Hostname and Network** screen of the wizard.
- To recover the backup to a host that differs from the source host, modify the **Client** field to specify the target host name.
- If you specify a different client, the recovered host uses the same hostname and IP settings as the source computer. This can cause hostname and IP address conflicts if the source computer is running on the same network.
- c. Click **Next**.
8. On the **Select System Recovery** screen, select the system backup that you wish to recover, and then click **Next**.
- System backups appear in descending order from most recent to oldest.
9. Review the **Save Sets to Restore** screen and click **Next**.
- The recovery process reformats critical volumes. The recovery process reformats non-critical volumes only if the disk signature on the target disk differs from the original disk.
- For example, if the disk was replaced.
- To perform a quick format instead of a full format operation, select **Perform a quick format of disks**.

#### Note

A quick format is much faster than full format but does not verify each sector on the volume.

The recovery process does not recover non-critical volume data. The topic, *Recovering file system data*, provides more information.

10. On the **System Recovery Summary** screen, select **Options** to display the **Non-Default Recover Options** screen.
11. On the **Non-Default Recover Options** screen:
- a. In the **Additional Options** field, type any required non-default options with their corresponding values. Non-default options are primarily used for troubleshooting purposes.
  - b. Click **OK** to save and close the **Non-Default Recover Options** screen and return to the **System Recovery Summary** screen.
  - c. Click **Restore** to begin the recovery process.,
12. On the **Confirmation** screen, click **OK**.

#### NOTICE

All data is lost on all volumes reformatted by the recovery process.

After the data recovery completes, the wizard writes the recovery log files to volumes in the Default backup pool. If you do not have a volume available, then the recovery operation appears to hang until media for the Default pool becomes available.

#### **Note**

You can cancel the log file backup without affecting the recovery operation.

13. Once the wizard and log files complete, click either **Reboot** or **Exit** as appropriate:

- Click **Reboot** to reboot the system and restore the application data. If you are recovering an Active Directory domain controller, it is recovered in non-authoritative mode by default.
- Click **Exit** if you need to recover a domain controller in authoritative mode. The computer returns to the WinPE command prompt. Boot into Directory Services Restore Mode (DSRM).

## Post-recovery tasks

The following sections provide information about recovering data that was not recovered in the Windows BMR operation.

### Using NMM for post-recovery tasks

If the recovered host has applications protected with NMM, all application-recovery operations must be performed by using the NMM client interface. The NMM documentation provides information on the post-recovery operations.

Before proceeding to the NMM documentation, ensure that the following conditions are met:

- After the recovery has completed and the system is rebooted, check the host's disk and volume configuration. All disks and volumes should appear as they did on the original system. However, if disk signatures do not match the original disks, non-critical disks might be offline or unmounted. In this case, you should use Microsoft Disk Manager to bring online or mount the disks. After the disks are online, a reboot operation should result in disk drive letter reassessments. If this correct drive letter assignments do not occur, manually assign drive letters to non-critical disks as needed. Non-critical volumes accessed by mount points might have similar issues.
- To completely recover the host, you might have to perform additional online recovery steps by using the NetWorker User program.
- If a folder is encrypted in Windows, for example, by selecting **Folder Properties > Advanced > Encrypt contents to secure data**, it is recovered as encrypted. However, the encryption attribute is not be set on the folder. You can manually reset the encryption attribute after the recovery operation. This is a Microsoft limitation.
- Windows BMR supports backup and recovery of files and folders encrypted with Windows Encrypting File System (EFS), and volumes encrypted with BitLocker. After BMR, the EFS or BitLocker services might be running but the EFS encryption attributes on files or folders must be re-enabled and BitLocker volumes must be re-encrypted. Consult Microsoft documentation for steps to encrypt with EFS and BitLocker.

#### **NOTICE**

You cannot install the NetWorker software on volumes that are encrypted with Microsoft BitLocker.

## Using an application backup tool other than NMM

If you backed up a database application with an application backup tool other than NMM, perform the following post-recovery operations:

- Recover any required file system data by completing the steps in the topic, *Recovering file system data*.
- Recover the application data by using the application backup tool, such as NetWorker User for SQL Server, NME, or any third-party application backup tool. Refer to the documentation that comes with your application backup tool.

### Recovering file system data

Perform an online recovery of any required user data on non-critical volumes. In some cases, user data on non-critical volumes needs to be recovered, for instance, when disk hardware was replaced due to a disaster prior to the Windows BMR operation.

#### Procedure

1. Manually remount any non-critical volumes as needed.
2. Start the NetWorker User program by using the `winworkr` command with the `-s` option to connect to the NetWorker server that backed up the source client data:

For example: `winworkr -s server_name`

If the `-s` option is not used and there is only one server detected, that server is connected automatically. If there are no servers detected or if there is more than one server available, the Change Server dialog box appears, allowing you to choose the server.

3. Click **Recover** to open the **Source Client** dialog box.
4. Select the source client, and then click **OK**.
5. Select the destination client for the recovered data, and click **OK**.
6. In the **Recover** screen, select the files to recover.
7. Click **Start** to begin the directed recovery.

The following sources provide more information:

- The topic, *Recovering Filesystem Data*, provides more information about recovery options.
- The NetWorker SolVe Desktop provides more information about an Active Directory online recovery and Windows Server Failover Cluster online recovery.
- The topic, *Backing Up and Restoring a Microsoft DFS*, provides more information about a DFSR online recovery.

## Performing post-recovery tasks for Active Directory services

The offline recovery of the DISASTER\_RECOVERY:\ save set in the case of a domain controller is non-authoritative. If a non-authoritative recovery is desired, then no additional steps are required. However, if you need to perform an authoritative recovery, follow these steps.

#### Procedure

1. On the **System Recovery Results** screen of the NetWorker Bare Metal Recovery wizard, select **Exit** to exit the wizard so that you can boot into Directory Services Restore Mode (DSRM).

Do not select **Reboot** in the wizard. Failure to boot into DSRM mode results in a non-authoritative recovery. If this occurs, run the Windows BMR wizard again and ensure that you boot into DSRM mode.

The WinPE command prompt appears.

2. At the WinPE command prompt, type the following **bcdedit** commands.

- a. Add a boot loader entry to force the system to boot into DSRM

```
X:\>bcdedit /copy {default} /d "Directory Service Repair Mode"
```

A message similar to the following appears:

```
The entry was successfully copied to  
{00000000-0000-0000-0000-000000000000}
```

The numbers and dashes in the previous message form a Globally Unique Identifier (GUID) that identifies a new entry. In this example, the GUID is for illustration purposes only. The actual GUID that is generated when you run the command is unique.

- b. Using the generated GUID, type the following command to set the safeboot option for the bootloader entry in the BCD store:

```
X:\> bcddedit /set {GUID_value} safeboot dsrepair
```

where **GUID\_value** is the GUID displayed by the previous **bcddedit** command.

- c. Exit the **bcddedit** command prompt to reboot the system.

Failure to boot into DSRM results in a non-authoritative recovery.

3. (Optional) If you have WINDOWS ROLES AND FEATURES save set backups and they are more recent than the DISASTER\_RECOVERY:\ save set, you can recover them in DSRM by using the NetWorker User program.
4. From the Windows command prompt, run the Windows **ntdsutil** utility.

The **ntdsutil** prompt appears. The **ntdsutil** utility is a command interface similar to the NetWorker recover interface. For help with the **ntdsutil** utility, type:

```
NTDSUTIL: ?
```

5. At the **ntdsutil** prompt, type:

```
NTDSUTIL: activate instance ntds  
NTDSUTIL: authoritative restore
```

6. To perform an authoritative recovery of a subtree or individual object, type:

```
NTDSUTIL: restore subtree "distinguished_name"
```

For example:

```
NTDSUTIL: restore subtree  
"OU=engineering,DC=Seattle,DC=jupiter,DC=com"  
NTDSUTIL: restore subtree  
"CN=mars,CN=users,DC=Seattle,DC=jupiter,DC=com"
```

The Microsoft Windows Server Resource Kit documentation on Active Directory provides information.

7. Exit the **ntdsutil** utility by typing **quit** at each successive **ntdsutil** prompt until the command prompt appears.

8. Type the following WinPE command at the Windows command prompt so that the host does not boot into DSRM mode upon reboot.

```
C:\> bcdedit /deletevalue safeboot
```

9. Restart the domain controller in normal mode and then log in and verify that the authoritative changes are replicated to the Active Directory replication partners.

## **Performing post-recovery tasks for hosts with Windows server roles that use SQL Server**

### **Procedure**

1. On node A, rebuild the SQL server by running the following Setup command:

```
C:\> Setup /QUIET /ACTION=REBUILDDATABASE /
INSTANCENAME=Instance_name /SQLSYSADMINACCOUNTS=domain_name
\administrator
```

The Setup tool is located on the SQL Server installation media and must be run from the command prompt with Windows Administrator privileges. Before you run this command, ensure that the SQL group is offline except for the shared disks.

The following Microsoft URL provides more information:

[http://msdn.microsoft.com/en-us/library/ms189302\(SQL.105\).aspx](http://msdn.microsoft.com/en-us/library/ms189302(SQL.105).aspx)

2. Bring the SQL sever services online.
3. Recover the SQL system databases (master, model, msdb) with NetWorker User for SQL Server, or a third-party application.

## **Performing post-recovery tasks for a Microsoft Hyper-V virtual machine**

Use NMM to restore your Hyper-V virtual machines.

## **Performing a BMR from a Physical Computer to a Virtual Machine (P2V)**

This section describes the process of restoring a NetWorker backup of a physical computer to a virtual machine (P2V).

P2V is supported for physical computers running the following operating systems:

- Microsoft Server 2008
- Windows Server 2008 R2
- Windows Server 2012
- Windows Server 2012 R2

P2V is supported when restoring to virtual machines created with the following hypervisors:

- Microsoft Hyper-V Server 2008 R2
- Microsoft Hyper-V Server 2012
- Microsoft Hyper-V Server 2012 R2
- VMware ESX 5.1
- VMware ESX 5.5
- VMware ESXi 5

### Procedure

1. Perform a backup of the physical computer as described in *Performing a Windows BMR backup*.
2. On the computer that runs your hypervisor, create a target virtual machine (VM).  
For VMware hypervisors, use a Windows Server 2008 R2 template as the guest operating system when you create the VM.
  - a. Configure the VM to use a virtual network adapter.
  - b. On the **VM configuration** page, select the LSI Logic SAS SCSI controller. Configure the disks on the VM to match the original physical computer configuration.
    - Create the same number of physical disks. Extra disks can be added after the P2V recovery.
    - The SCSI disk numbers must match the original disk numbers.
    - The VM disk sizes must match, or exceed, the original disk sizes.
3. On the VM, boot the WinPE ISO which starts the BMR wizard. Refer to *Creating a Windows BMR bootable image* for more information.
4. On the VM, use the BMR wizard to configure the hostname and network configuration.
  - a. On the **Select Server** screen, ensure that you specify the name of the physical computer as the NetWorker client.
  - b. On the **Select Backup** screen, select the backup to restore. Backups are listed in chronological order with the most recent backup first.
  - c. On the **Summary** screen, if the save set was created with NetWorker 8.1 or earlier, select the **Restore physical computer to virtual machine (P2V)** checkbox.  
If the **Restore physical computer to virtual machine (P2V)** checkbox is not marked, the VM might not boot successfully after the restore is complete.
  - d. Select **Restore** to start the restore.
5. Reboot the VM when the P2V BMR is complete.

## Performing Post-P2V tasks

The following section provides information about additional tasks that are required after a P2V recovery.

### Procedure

1. If you are running VMware, install VMware tools.
2. Use **Device Manager** to remove disabled NIC devices.

This is required because the original network adapter is no longer available. It can also be required for other devices.

To remove disabled devices:

- a. From Device Manager, select the Show Hidden Devices option.
- b. Select the hidden NIC device.
- c. Select uninstall.
3. Configure the virtual network adapter to restore network connectivity.

## Troubleshooting Windows BMR

The following topics provide information to help troubleshoot Windows BMR operations.

### Performing a manually uninstall and reconfigure of a NIC on Windows 2012

If the guest operating system is Windows 2008 R2, the NIC settings are retained by the P2V BMR. However, if the guest operating system is Windows 2012 then Windows performs some Plug-N-Play configuration during the post-BMR reboot. This activity disables the original NIC and creates a new NIC.

1. In the **Device Manager** select **Display disabled devices** > **Uninstall the disabled NIC**.
2. Configure the new NIC with the desired network settings.

### Recovering and viewing Windows BMR log files

#### **Windows BMR log files**

To help troubleshoot an unsuccessful recovery, the following log files are generated and backed up during the Windows BMR operation:

- **daemon.raw** — This is the same as **daemon.log** for monitoring services.
- **Ossr\_director.raw** — Contains the recovery workflow of the **DISASTER\_RECOVERY:\ save set**. This log also contains any errors related to recovering the save set files or Windows ASR writer errors.
- **recover.log** — Contains output from the NetWorker recover.exe program. This information is generated during the recovery of each save set. This log also contains messages about errors related to critical volume data recovery.
- **WinPE\_Wizard.log** — Contains information about the work flow related to the NetWorker Bare Metal Recovery wizard user interface.
- **winpe\_nw\_support.raw** — Contains output from the **winpe\_nw\_support.dll** library. The output provides information about the communication between the NetWorker Bare Metal Recovery wizard and the NetWorker server.
- **winpe\_os\_support.log** — Contains output information related to Microsoft native API calls.

If the Windows BMR fails, you can recover the log files by using FTP on the recovery host or by using a directed recovery. If the Windows BMR was successful, you can recover the log files directly to the recovered host.

To view log files, you can use either a text editor or the **nsr\_render\_log** program, depending on the log file format.

#### **Accessing the log files using FTP**

1. Access the WinPE command line on the recovery host.  
You might have to exit the Windows Bare Metal Recovery wizard to access the WinPE command line. If you exit the wizard, do not reboot.
2. Disable the Windows firewall. For example:

```
X:\Program Files\EMC Networker\nsr\wizard> wpeutil DisableFirewall
```

By default, the Windows firewall is enabled on WinPE, and this blocks the FTP port from transferring files.

3. Change to the following directory that contains the log files:

```
X:\Program Files\EMC Networker\nsr\logs
```

4. Use the FTP utility to move the log files to another NetWorker host.

#### Accessing log files using a directed recovery operation

1. Start the NetWorker User program by using the **winworkr** command with the **-s** option to connect to the NetWorker server that backed up the source client data:

```
winworkr -s server_name
```

If the **-s** option is not included, and there is only one server detected, that server is connected automatically. If there are no servers detected or if there is more than one server available, the Change Server dialog box appears, allowing you to choose the server.

2. Click **Recover** to open the **Source Client** dialog box.
3. Select the source client, which is the client that was being recovered, and click **OK**.
4. Select the destination client for the recovered data, and click **OK**.
5. From the **Options** menu, select **Options**, specify a folder location in which to relocate the recovered log files, and then click **OK**.
6. In the **Recover** window, select the log files to recover.  
The log files are typically located in the following directory:

```
X:\Program Files\EMC Networker\nsr\logs
```

7. Click **Start** to begin the directed recovery.

The topic, *Recovering Filesystem Data*, provides more information about the permissions required for directed recoveries.

#### Viewing the log files

Use a text editor to view the following log files:

- recover.log
- WinPE\_Wizard.log

Use the nsr\_render\_log program to view the following log files:

- Ossr\_director.raw
- winpe\_nw\_support.raw

For example, type the following command at a command prompt to display the Ossr\_director.raw file:

```
c:\> nsr_render_log "C:\logs\Client-bv1\Ossr_director.raw"
```

To direct the Ossr\_director.raw file to a text file that can be viewed in a text editor, type the following:

```
c:\> nsr_render_log "C:\logs\Client-bv1\Ossr_director.raw" > mylog.txt
```

## BMR backup fails when System Reserved Partition is offline

BMR backups may fail with the following error:

```
device is not ready
```

Windows 2008 R2 Server has 100 MB reserved as the System Reserved Partition. When backing up the system state, VSS includes the System Reserved Partition (used for BitLocker and Boot files), but the backup fails because the System Reserved Partition is offline. This can occur if the Windows automount capability is disabled. Although there are circumstances where the automount capability must be disabled, it can result in the partition being offline after a reboot. Automount must be enabled for a BMR backup to succeed.

To work around this issue, use either of the following solutions:

### Solution 1

From the command prompt, run DISKPART with the following commands:

```
C:\>DISKPART
C:\DISKPART> List volume
C:\DISKPART> Select volume <number of 100 MB system partition>
```

C:\DISKPART> Online volume (if the volume is offline)

The volumes can go offline if automount is disabled while using 3rd party storage software or if the user manually disabled the automount for the volume.

This Microsoft article provides details on preventing volumes from going offline by checking and setting the system automount attribute, KB2419286: <http://support.microsoft.com/kb/2419286>

### Solution 2

From the Disk Management console:

1. Access Disk Management, open command prompt:

```
C:\>Diskmgmt.msc
```

2. Assign the drive letter to the 100 MB partition to bring the disk online:
  - a. Right click the 100 MB volume and select **Change Drive Letter and Paths....**
  - b. Assign a new drive letter to the volume.

Assigning the drive letter ensures that the volume will be online after a reboot.

## Wizard cannot locate the NetWorker server or DNS server

If the NetWorker Bare Metal Recovery wizard cannot locate the NetWorker server or the DNS server (if one is being used), try the following:

- If you are using a local hosts file instead of a DNS server, verify that the hostname and IP address of the NetWorker server and Avamar deduplication node (if one is being used) was entered correctly.
- If you are using a DNS server, verify that the values entered in the Configure Hostname and Network screen, were entered correctly.
- Verify that the NetWorker server was correctly specified in the Select NetWorker Server screen.

To verify hostname and IP address values, use the ping utility that is included in the WinPE environment:

1. Exit the **NetWorker Bare Metal Recovery** wizard but do not reboot the host. You are returned to the WinPE command line.
2. Use the **ping** utility to locate and verify hostnames and IP addresses. For example:

```
X:\Program Files\EMC Networker\nsr\wizard>ping -a hostname
```

3. Restart the wizard. For example:

```
X:\Program Files\EMC NetWorker\nsr\wizard> javaw -jar  
WinPEWizard.jar
```

---

**Note**

After the wizard has been restarted, you can switch between the wizard and the WinPE command line without exiting the wizard.

## Multiple NICs cause errors in locating the NetWorker server

An error message similar to the following might appear when you try to recover a host with multiple NICs:

```
Error retrieving the list of Networker servers
```

This is an indication that the NIC selected by the wizard is not the NIC that was connected to the NetWorker server when the backup was performed and the NIC might not have connectivity to the server. This applies when searching for an available server or specifying a specific server. To resolve the issue, select another NIC.

## Network configuration values might not be retained after reboot

In some cases, a host does not retain its network configuration data after a Windows BMR operation and after the host boots. If the recovered host is experiencing network connectivity issues, confirm that network properties for the local connections are correct. If necessary, manually update the network configuration data on the host.

## VSS backups fail because a critical disk is offline

VSS backups fail if a critical volume is offline during the backup operation. You might be able to remedy the problem by following the steps outlined in the Microsoft Knowledgebase (KB) article 980794, which can be found at:

```
http://support.microsoft.com/kb/980794
```

The patch mentioned in this KB article is most likely on your Windows system if it is kept up-to-date. In this case, you only have to create and populate the Registry keys as described in the article.

This issue is most often encountered when backing up a passive node in a MSCS cluster and a critical volume is not located on the physical host of the passive node but is instead located on the physical host of the active node.

## Jobquery fails to establish a connection with large scale jobs

Jobquery fails to establish a connection with the jobsDB when the jobsDB contains more than 3,00,000 records.

The workaround is to run *nsradmin* from the command line with the following parameters:

```
nsradmin -S [jobsdatabase path]
```

## Additional recovery options

You can specify non-default recovery options on the WinPE command line or in the Additional Options field of the NetWorker Bare Metal Recovery wizard.

The following table describes the additional recovery options that can be used with a Windows BMR operation.

**Table 110** Additional recovery options

| Entry                                                                                                                  | Result                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |
|------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>-D n</b><br>where n is a number from 1 to 9, with 9 providing the most debug information and 1 providing the least. | Additional debug information is included in the Windows BMR log files.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |
| <b>-v</b>                                                                                                              | Additional information on the progress of the recovery displays in the wizard's System Recovery Status window.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |
| <b>-p</b>                                                                                                              | <p>By default, the Windows BMR recovery skips the formatting of non-critical disks.</p> <p>By using the <b>-p</b> option, any existing partitions are deleted and all disks are reformatted on the recovered computer to match the layout of the system image. However, by Microsoft specification, even if the <b>-p</b> option is selected, a non-critical volume is not reformatted if the disk signature has not changed since the backup.</p> <p>This option might be useful in situations where a system fails to recover because of disk mismatch errors. In this case, the <b>-p</b> option might resolve those errors.</p> <p>The recovery process does not recover non-critical volume data even if the volume is reformatted. Non-critical volumes can be recovered by using the NetWorker User program after the wizard has completed and the host has been rebooted.</p>                           |
| <b>recover -s &lt;NetWorker server&gt; -U -N "WINDOWS ROLES AND FEATURES \Cluster Database"</b>                        | <p>When the restored data is meant to override the data on other nodes, it should be restored using the authoritative mode. Once this data is restored to one of the nodes, it is propagated to the other nodes and overwrites any newer data on those nodes.</p> <p>Perform Authoritative restore by using the command on the left. While the recovery is in progress, observe that the status of the groups change from Online to Pending to Offline in the Failover Cluster Management application. Alternatively, check the Event Viewer, under <b>Application and Services Logs &gt; Failover Clustering &gt; Operational</b> on all nodes that the Cluster Service has stopped and restarted.</p> <p>Recover the shared drive data through <i>winworkron</i> the cluster node with its current active node. Select source client as virtual client and destination client as the current active node.</p> |

## Reboot Required after Recovery Operation

Newly recovered NetWorker client computers running Windows Server 2012 R2 can require an extra reboot to restore access to application icons, previously viewable on the desktop.

# CHAPTER 25

## Volume Shadow Copy Service

This chapter contains the following topics:

- [Overview of VSS](#)..... 650
- [VSS and the backup process](#)..... 650
- [Controlling VSS from NetWorker software](#)..... 653

## Overview of VSS

If the NetWorker Module for Microsoft is installed on the client computer, information in this chapter may be superseded by information in the NetWorker Module for Microsoft documentation. The *EMC NetWorker Module for Microsoft Administration Guide* provides more information about the NetWorker Module for Microsoft.

Volume Shadow Copy Service (VSS) is a Microsoft technology that acts as a coordinator among all the components that create, archive, modify, back up, and restore data, including:

- The operating system
- Storage hardware
- Applications
- Utility or backup programs, such as NetWorker software

VSS allows for the creation of a point-in-time snapshot, or temporary copy, of a volume. Instead of backing up data directly from the physical file system, data is backed up from the snapshot. In addition, VSS allows for a single, point-in-time capture of the system state.

NetWorker uses VSS technology to create snapshot backups of volumes and exact copies of files, including all open files. Databases and files that are open due to operator or system activity are backed up during a volume shadow copy. In this way, files that have changed during the backup process are copied correctly.

Shadow copy (snapshot) backups ensure that:

- Applications can continue to write data to the volume during a backup.
- Open files are not omitted during a backup.
- Backups can be performed at any time, without locking out users.

---

### Note

VSS backups do not use snapshot policies, which are required to perform snapshot backups. The Snapshot Integration Guide documentation provides more information.

---

## VSS and the backup process

In VSS terms, NetWorker software is a requestor — an application that needs data from other applications or services. When a requestor needs data from an application or service, this process occurs:

1. The requestor asks for this information from VSS.
2. VSS reviews the request for validity.
3. If the request is valid and the specified application has the requested data, the request goes to the application-specific writer, which prepares the requested data.

Each application and service that supports VSS has its own writer, which understands how the application or service works:

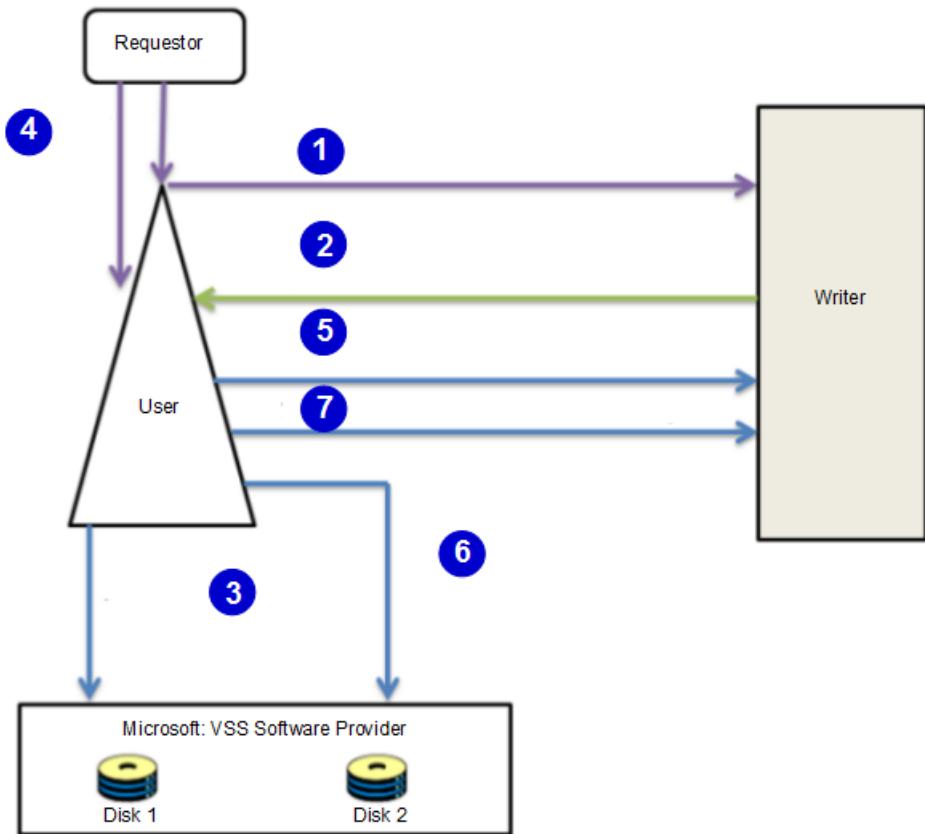
1. After the writer signals that it has prepared the data, VSS directs the writer to freeze I/O to the selected volumes, queuing it for later processing.
2. VSS then calls a provider to capture the requested data.

3. The provider, which is either software-based or associated with particular hardware (for example, a disk array), captures the prepared data, creating a snapshot (or shadow copy) that exists side-by-side with the live volume. [Provider support on page 652](#) contains more information.

The process of creating a snapshot involves interaction with the operating system. The amount of time it takes to create a snapshot depends on a number of factors, including the writer activity taking place at the time. Once the snapshot is created, the provider signals VSS, which tells the writer to resume activity. I/O is released to the selected volumes and any queued writes that arrived during the provider's work are processed.

The following figure provides a graphical representation of the VSS backup process.

**Figure 39** VSS backup process



This figure provides a graphical representation of the VSS backup process:

1. NetWorker software (the requestor) asks VSS to enumerate writers and gather their metadata.
2. Writers provide an XML description of backup components and define the recover method.
3. VSS asks which providers can support a snapshot for each of the required volumes.
4. Requestor asks VSS to createsnapshot.
5. VSS tells the writers to freeze activity.
6. VSS tells the providers to create the snapshot of the current state on disk.

VSS tells the writers to resume activity.

**Figure 39** VSS backup process (continued)

NetWorker software backs up data from the point-in-time snapshot that is created during this process. Any subsequent data access is performed on the snapshot, *not* the live (in-use) file system. The requestor has no direct contact with the provider; the process of taking a snapshot is seamlessly handled by VSS. Once the backup is complete, VSS deletes the snapshot.

## Provider support

By default, the NetWorker client always chooses the Windows VSS system provider for backups. If you want to use a hardware provider or a specific software provider for a particular NetWorker client, enter the following command in the NetWorker client resource Save Operations attribute:

```
VSS:VSS_ALLOW_DEFAULT_PROVIDER=yes
```

When the previous command is specified for a NetWorker client, a backup provider is selected based on the following default criteria as specified by Microsoft:

1. If a hardware provider that supports the given volume on the NetWorker client is available, it is selected.
2. If no hardware provider is available, then if any software provider specific to the given NetWorker client volume is available, it is selected.
3. If no hardware provider and no software provider specific to the volumes is available, the Microsoft VSS system provider is selected.

[Controlling VSS from NetWorker software on page 653](#) provides more information about specifying VSS commands for a NetWorker client. [VSS commands on page 655](#) provides information about other VSS commands.

**NOTICE**

Windows Bare Metal Recovery backups always use the Windows VSS system provider even if the VSS:VSS\_ALLOW\_DEFAULT\_PROVIDER=yes command is specified for the NetWorker client resource.

## Troubleshooting hardware providers

If you have specified the VSS:VSS\_ALLOW\_DEFAULT\_PROVIDER=yes command as described in [Provider support on page 652](#) and the hardware provider and NetWorker are incompatible, try one of the following workarounds:

- Uninstall the hardware provider.
- Migrate any data that is backed up by the NetWorker client to a disk LUN (Logical Unit Number), such as C:\, that is not controlled by a hardware provider. In this way, the NetWorker client will backup all data using the software provider.

Be aware that if the NetWorker Module for Microsoft is installed on the client host, then the previously mentioned workarounds may not be required. Refer to the NetWorker Module for Microsoft documentation for details.

## The importance of writers

Writers play an important role in properly backing up data. They provide metadata information about what data to back up, and specific methods for properly handling components and applications during backup and restore. They also identify the type of

application or service that is being backed up, for example System Boot or System Services. Writers do *not* play a role in backing up the file system.

Writers are currently only available for active services or applications. If a service or application is present on a system but is not active, information from its writer will not be available. Consequently, a writer can appear or disappear from backup to backup.

In addition, NetWorker software maintains a list of supported writers in the NSRLA database of the client machine. When backing up data, the software checks to ensure that these conditions exist:

- The writer associated with the application is present on the system and active.
- The writer appears on the list of supported writers in the NSRLA database.
- A user has not disabled the writer.

If these conditions are all true for a particular writer, NetWorker software defaults to backing up data by using VSS technology. If any of the conditions are false for a particular writer, the data served by that writer is excluded from the backup operation.

## List of supported writers

During a VSS backup operation, NetWorker software validates each writer against a list of supported writers. As part of a software release, or between releases, there may be updates to the list of supported writers. The *EMC NetWorker Software Compatibility Guide* provides a list of the currently supported writers.

# Controlling VSS from NetWorker software

By default, NetWorker uses VSS technology to back up a client. For VSS SYSTEM save sets, this means NetWorker software uses VSS for most save sets and writers. For the file system, this means the software attempts to take a snapshot of each drive, but if it fails, then it saves the file system by using the legacy method (that is, no snapshot is taken). During a given backup for an individual client, either the VSS method or the legacy method is used, but not both.

There may be times when you need finer control over how NetWorker software uses VSS. For example, if you need to disable VSS. You can control VSS from the Administration window, the NetWorker User program, or the command prompt.

These sections provide more information:

- [Controlling VSS from the Administration window on page 653](#) provides details on how to control VSS from the Administration window.
- [Control VSS from the command-prompt on page 654](#) provides details on how to control VSS from the command prompt.
- [Globally disabling VSS on page 654](#) provides details on how to disable VSS globally.

## Controlling VSS from the Administration window

### Procedure

1. From the Administration window, click **Configuration**.
2. Click **Clients**.
3. Right-click the client for which you want to control VSS, then select **Properties**. The **Properties** dialog box appears, with the **General** tab displayed.
4. Click the **Apps & Modules** tab.

5. In the **Save Operations** attribute, type the appropriate command, then click **OK**.

- Separate multiple commands with a semicolon (;).
- If the **Save Operations** attribute is left blank, NetWorker software backs up data by using VSS.

## Notes:

- The **Save Operations** attribute does not support NetWorker Module save sets. If a NetWorker Module save set name is entered in the window, the backup fails.
- If you enter a VSS command in the **Save Operations** attribute of the **Administration** window, the command runs when the client backup is started as part of a save set.
- Use the **Save Operations** attribute only for clients running NetWorker software release 7.2 or later. If anything is entered in this attribute for a client that is running an earlier NetWorker software release, the backup will fail.

## Control VSS from the command-prompt

You can control VSS from the command-prompt on a NetWorker client or the NMC server by using the -o option and the Save Operations commands, but only while performing a save, savefs, or nsrarchive operation.

For example, to completely disable VSS while backing up C:\myfile to the server jupiter, type:

```
save -s jupiter -o "vss:=off" "C:\myfile"
```

Although the server name is not required in the preceding command example, include the name to ensure that the save command finds the correct server. Separate multiple Save Operations commands with a semicolon (;).

The *EMC NetWorker Command Reference Guide* provides more information about the save, savefs, and nsrarchive commands.

### Note

If you change the VSS setting on a client by using the Local Save Operations dialog box or the command prompt, it does not affect that client's VSS setting on the server. Likewise, if you change a client's VSS setting on the server, it does not affect the Local Save Operations setting or the command-prompt VSS setting on the client.

## Globally disabling VSS

Use the nsradm program to disable VSS for all clients globally or only for clients with a certain Windows operating system.

To disable VSS:

### Procedure

1. Log in as root or as Windows Administrator on the NetWorker server.

To disable VSS for all NetWorker clients:

- a. Create an input file for the nsradm command. The input file will eliminate interactive prompting as each client gets updated. For example, create a text file named disable-vss.txt and type the following into the file:

```
show name; client OS type; Save operations
print type: NSR client
```

```
update Save operations: "VSS\*:*=off"
print
```

To disable VSS only for clients on a particular Windows operating system such as Windows NT:

- b. Create an input text file, for example, create a file named disable-vss-nt.txt and type the following into the file:

```
show name; client OS type; Save operations
print type: NSR client; client OS type: "Windows NT Server on
Intel"
update Save operations: "VSS\*:*=off"
print
```

2. Type either of the following at the command prompt:

```
nsradmin -i <path>\disable-vss.txt
nsradmin -i <path>\disable-vss-nt.txt
```

where <path> is the directory location of the input file.

## VSS commands

This section lists the commands and syntax used to control VSS. [Controlling VSS from NetWorker software on page 653](#) describes how to enter these commands in NetWorker.r

**Table 111** VSS Save operation attribute values

| Task                                                                                      | Save operations attribute          | Behaviour                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             |
|-------------------------------------------------------------------------------------------|------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| To enable VSS.                                                                            | Blank                              | Leaving the attribute empty will result in NetWorker software automatically using VSS.                                                                                                                                                                                                                                                                                                                                                                                                                |
| To completely disable VSS.                                                                | VSS:*=off                          | <p>VSS backups will not occur and backing up the following save sets for a NetWorker client resource will yield these results:</p> <ul style="list-style-type: none"> <li>• DISASTER_RECOVERY:\ save set<br/>Backup will fail at the beginning of backup operation.</li> <li>• All save set<br/>Backups will fail.</li> </ul>                                                                                                                                                                         |
| To use a hardware provider or a specific software provider for a NetWorker client backup. | VSS:VSS_ALLOW_DEFAULT_PROVIDER=yes | <p>A backup provider is selected based on the following default Microsoft criteria:<br/>If a hardware provider that supports the given volume on the NetWorker client is available, it is selected.<br/>If no hardware provider is available, then if any software provider specific to the given NetWorker client volume is available, it is selected.<br/>If no hardware provider and no software provider specific to the volumes is available, the Microsoft VSS system provider is selected.</p> |

**Table 111** VSS Save operation attribute values (continued)

| Task | Save operations attribute | Behaviour                                                                                                                                                                                                                                                                                                          |
|------|---------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|      |                           | Windows Bare Metal recovery backups always use the Windows VSS system provider even if the VSS:VSS_ALLOW_DEFAULT_PROVIDER=yes command is specified for the NetWorker client resource. <a href="#">Windows Bare Metal Recovery on page 611</a> provides more information about Windows Bare Metal recovery backups. |

# CHAPTER 26

## Networking and connectivity

This chapter contains the following topics:

- [Name resolution and connectivity](#)..... 658
- [Troubleshooting name resolution and connectivity errors](#)..... 658
- [Using multihomed systems](#)..... 666
- [NIC Teaming](#)..... 672
- [Using DHCP clients](#)..... 673

## Name resolution and connectivity

A NetWorker host must consistently and reliably connect to and resolve each destination NetWorker host by fully qualified domain name (FQDN), shortname, and IP address.

The NetWorker software requires consistent and predictable forward and reverse name resolution to work correctly. NetWorker performs name resolution checks during the following operations:

- NetWorker daemon startup.
- Client and Device resource configuration.
- Backup, recovery, and device operations.

NetWorker relies on the operating system to perform the following tasks:

- Handle name resolution requests.
- Resolve hostnames to IP addresses (forward name resolution lookups).
- Resolve IP addresses to hostnames (reverse name resolution lookups).

**NOTICE**

On Windows Server 2008 R2, EDNS0 queries increase the size of the DNS UDP packet and some firewalls block UDP packets larger than 512 bytes. EMC recommends that you disable EDNSprobes on hosts that operate in a firewalled environment, as a DNS Server or Domain Controller. To disable EDNSprobes, run the following command:

```
dnscmd /config /EnableEDNSProbes 0
```

---

NetWorker supports the use of Internet Protocol version 6 (IPv6) in a dual stack or in a pure IPv6 environment. NetWorker does not support NetWorker resource configurations that use temporary or link-local IPv6 addresses.

When a NetWorker host uses IPv6 addressing, ensure that you add the IPv6 address for the host in DNS Server or the hosts file and to the alias field in the client resource. The *EMC NetWorker Installation Guide* provides information about using NetWorker in an IPv6 environment.

## Troubleshooting name resolution and connectivity errors

When NetWorker operations fail due to name resolution issues, the following types of error conditions can appear in the daemon.raw file or in the savegroup completion report:

- RPC errors
- Unknown host errors
- Failures in contacting the portmapper
- Connection failures or time outs
- Unexpected exits by programs
- Connection refused errors
- Failure of a remote command (rcmd() function) to an active client
- Failures in name-to-address translation
- Program not registered errors
- Failures of NetWorker services to start

- Failures of NetWorker services to remain active
- Invalid path errors

When NetWorker operations fail due to name resolution issues, the following error messages can appear in the daemon.raw file or in the savegroup completion report:

- Host name for IP address IP\_address could not be determined through DNS
- IP address for host 'hostname' could not be determined through DNS
- Warning, cannot resolve host hostname to IP\_address, name server may be misconfigured.
- 'Client\_name': Couldn't look up the name of address:'NetWorker\_server\_IP':node name or service name not known.
- nsexec: nsexecd on (client) is unavailable. Using rsh instead
- nsexec: host hostname cannot request command execution permission denied
- Cannot connect to nsexecd on client NetWorker\_server .rhost permissions do not allow rsh permission denied

Before you can troubleshoot name resolution and connectivity issues, you must determine between which hosts the connection problems occurred. The problems can occur between any two types of NetWorker hosts, for example, between the NetWorker server and a client or between a client and a storage node.

Complete the following steps to troubleshoot name resolution and connectivity errors:

1. Document the steps you take and the results, especially error messages, in case you need to contact EMC Technical Support.
2. Use operating system tools to confirm that basic connectivity exists between the source and destination hosts. For example, **telnet**, **ping**, and **traceroute**. [Verifying basic connectivity on page 659](#) provides more information.
3. Check that the source and destination hosts consistently and correctly resolves all names and IP addresses for each host. [Verifying name resolution on page 661](#) provides more information.
4. Verify that the configuration of the source and destination host includes all relevant information for each host in the Aliases attribute and the servers file. [Verifying the NetWorker configuration on page 665](#) provides more information.

## Verifying basic connectivity

NetWorker requires reliable and consistent connectivity between the source and destination hosts. Confirm that you can remotely connect to the host. When the source and destination hosts reside on different networks, verify the network connectivity between the hosts.

### Verifying remote host connectivity

Try to connect to the host. If a backup fails for a NetWorker client, then try to connect to the client by using other tools. For example, try to connect to the host by using Remote Desktop Connection on Windows or the **telnet** command on UNIX. If remote connections to the host fail, then investigate external host connectivity issues.

### Verifying network connectivity

Use the **ping** command and the **traceroute** command on UNIX and Linux or the **pathping** command on Windows to transmit packets between hosts and verify that network connectivity exists between the source and the destination hosts. Run each

command from the source host and destination host and use each command with the shortname, FQDN, and the IP address of the destination host.

In the following example, the source host mnd.emc.com is a Linux host with the IP address 10.1.1.10. The destination host pwd.emc.com is a Windows host with the IP address 10.1.1.20.

### Procedure

1. On the pwd.emc.com host, run the following **pathping** commands:

```
pathping pwd.emc.com
pathping pwd
pathping 10.1.1.20
pathping mnd.emc.com
pathping mnd
pathping 10.1.1.10
```

A successful pathping command displays the following information:

```
C:>pathping mnd.emc.com
Tracing route to mnd.emc.com [10.1.1.10]
over a maximum of 30 hops:
    0  pwd.emc.com [10.1.1.20]
    1  mnd.emc.com [10.1.1.10]
Computing statistics for 25 seconds...
                Source to Here   This Node/Link
Hop  RTT      Lost/Sent = Pct  Lost/Sent = Pct  Address
    0          |                  |          |
[10.1.1.20]          0/ 100 =  0%  0/ 100 =  0%  pwd.emc.com
    1     0ms      0/ 100 =  0%  0/ 100 =  0%  mnd.emc.com
[10.1.1.10]
Trace complete.
```

An unsuccessful pathping command displays the following information:

```
C:>pathping 10.1.1.10
Tracing route to 10.1.1.10 over a maximum of 30 hops
    0  pwd.emc.com [10.10.10.20]
    1  *          *          *
Computing statistics for 0 seconds...
                Source to Here   This Node/Link
Hop  RTT      Lost/Sent = Pct  Lost/Sent = Pct  Address
    0          |                  |          |
[10.10.10.20]
Trace complete.
```

2. Complete the following steps on the mnd.emc.com host:

- a. Run the following **ping** commands:

```
ping pwd.emc.com
ping pwd
ping 10.1.1.20
ping mnd.emc.com
ping mnd
ping 10.1.1.10
```

- b. Run the following **traceroute** commands:

```
traceroute pwd.emc.com
traceroute pwd
traceroute 10.1.1.20
traceroute mnd.emc.com
traceroute mnd
traceroute 10.1.1.10
```

Ensure that each `ping` and `traceroute` command succeeds. Lost packets can indicate a slow connection between hosts. If any attempt to transmit a packet fails with an error message, then verify the name resolution and ensure that all routers between the source host and destination hosts are operational.

## Using `nsrrpcinfo` to report the status of registered RPC services

Use the `nsrrpcinfo` command to verify that you can establish sessions to the portmapper daemon on the source and destination host. The NetWorker Remote Exec service on Windows and the `nsreexecd` daemon on UNIX, starts the portmapper service that NetWorker uses.

Type the following commands on the source and destination host:

```
nsrrpcinfo -p hostname_of_NetWorker_server
nsrrpcinfo -pFQDN_of_NetWorker_server
nsrrpcinfo -pIP_address_of_NetWorker_server
nsrrpcinfo -pshortname_of_destination_host
nsrrpcinfo -pFQDN_of_destination_host
nsrrpcinfo -pIP_address_of_the_destination_host
```

### Note

On Windows, the `NetWorker_installation_dir\nsr\bin` contains the `nsrrpcinfo` program.

When the `nsrrpcinfo` command runs successfully, the output displays a list of port numbers and names. For example:

```
# nsrrpcinfo -p
  program vers proto   port
    100000    2   tcp    7938  nsrportmapper
    100000    2   udp    7938  nsrportmapper
    390436    1   tcp    7943  nsreexecd
    390435    1   tcp    9549  nsreexecd
    390113    1   tcp    7937  nsreexecd
```

Ensure that the correct program number appears for each NetWorker process. If you do not see the correct program number or the appropriate NetWorker ports, and a personal or external firewall exists between the source and the destination hosts, then review the NetWorker configuration port requirements. The *EMC NetWorker Security Configuration Guide* provides more information about how to configure NetWorker in a firewall environment and the correct program numbers for each NetWorker daemon.

## Verifying name resolution

When NetWorker performs name resolution lookups, NetWorker uses the first entry in the name resolution resource that matches the request. Name resolution services include: the resolver cache, DNS, LDAP/AD, and the hosts file. Name resolution lookups check the resolver cache first. Entries that appear in the cache do not reflect changes made to the host tables and on the DNS server until a cache flush occurs.

A cache flush occurs for the following hosts:

- All hosts in the cache at intervals defined by the operating system, by system-specific commands, or by reinitialization of network components, including a reboot.
- A specific host in the cache each time that you use the operating system command `nslookup` to resolve the hostname.

## Determining the IP name search order

NetWorker relies on the operating system to determine the order in which to check name resolution services. Before troubleshooting a possible name resolution error, determine the search order used by the operating system.

The name resolution search order differs for each operating system:

- Linux, Solaris, and HP-UX operating systems use the hosts database entry in the `/etc/nsswitch.conf` file to define the name resolution search order. For example, when the operating system checks the DNS Server and then the `hosts` file, the `nsswitch.conf` entry appears as follows:
 

```
hosts: dns files
```
- AIX operating systems use one of three methods to select the name resolution search order:
  - The `NSORDER` environment variable. For example, when the operating system checks the `hosts` file first and then DNS, the `NSORDER` environment variables appears as follows:
 

```
NSORDER=local,bind4
```
  - The hosts database entry in the `/etc/netsvc.conf` file. For example, when the operating system performs name resolution checks by using the DNS Server and then the `hosts` file, the `hosts` entry in the `netsvc.conf` file appears as follows:
 

```
hosts=local,bind4
```
  - The `/etc/irs.conf` file. For example, when the operating system checks the `hosts` file first and then the DNS (IPv4 address), the `hosts` entries in `irs.conf` file appear as follows:
 

```
hosts local
hosts dns4
```

---

### Note

The `NSORDER` environment variable setting overrides the settings in the `/etc/netsvc.conf` file and the `/etc/irs.conf` file. The `/etc/netsvc.conf` file setting overrides the `/etc/irs.conf` file setting.

- Windows Server 2008 R2 operating systems use the following search order: WINS, network broadcast, `LMhosts` file, `hosts` file, then DNS. Windows Server 2008 and earlier operating systems use a similar search order with the exception that the network broadcast occurs before the WINS lookup.

## Verifying correct hosts file resolution

The operating system provides NetWorker with the first entry in the `hosts` file that matches the name resolution requirement. Additional instances of an IP address, FQDN, or shortname that appear in the `hosts` file for a host are ignored when NetWorker attempts to resolve names.

When you create or modify the `hosts` file, ensure that you:

- Specify each hostname or IP address only once.

- Specify each FQDN and alias for a host on the same line as the IP address. For example:

```
IP address Canonical name FQDN alias alias...
```

- Specify the IPv6 loopback interface (::1) with the localhost on Linux and UNIX, when the operating system configures the IPv6 loopback interface. For example:

```
::1 localhost  
127.0.0.1 localhost
```

#### Note

The IPv6 loopback entry must remain in the `hosts` file when the host exists in a pure IPv4, pure IPv6, or dual stack configuration.

## Using the nslookup command

Use the `nslookup` command to verify that each DNS Server used by the source and destination hosts, correctly and consistently resolves both hosts by the short name, FQDN, and IP address.

Perform the following steps on the source host and destination host.

#### Procedure

- Determine the Primary and Secondary DNS Servers that the host uses for name resolution:
  - On UNIX, review the `/etc/resolv.conf` file.
  - On Windows, type the following command from a command prompt:  
`ipconfig /all`
- Use the `nslookup` command in interactive mode to validate forward name resolution lookups with the Primary DNS Server:
  - From a command prompt, type: `nslookup`
  - At the `nslookup` command prompt, specify the following values:

```
Shortname_of_source_host  
Shortname_of_source_host  
Shortname_of_source_host  
FQDN_of_source_host  
FQDN_of_source_host  
IP_address_of_source_host  
IP_address_of_source_host  
IP_address_of_source_host  
Shortname_of_destination_host  
Shortname_of_destination_host  
Shortname_of_destination_host  
FQDN_of_destination_host  
FQDN_of_destination_host  
FQDN_of_destination_host  
IP_address_of_destination_host  
IP_address_of_destination_host  
IP_address_of_destination_host
```

**Note**

EMC recommends that you resolve every name and IP address for each host three times to ensure that successive queries return correct and consistent values.

3. Complete the following steps when the host uses multiple DNS Servers for name resolution:

- a. Change the DNS Server that **nslookup** uses for name resolution.

In this example, the `ipconfig /all` command on a Windows host returns two DNS Servers, the Primary DNS Server 10.5.5.10 and secondary DNS Server 10.5.5.11.

To configure **nslookup** to use the IP address 10.5.5.11, type the following commands:

```
C:\>nslookup
Default Server: lad.emc.com
Address: 10.5.5.10
> server 10.5.5.11
Default Server: dmd.emc.com
Address: 10.5.5.11
```

- b. At the **nslookup** command prompt, specify the following values:

```
Shortname_of_source_host
Shortname_of_source_host
Shortname_of_source_host
FQDN_of_source_host
FQDN_of_source_host
FQDN_of_source_host
IP_address_of_source_host
IP_address_of_source_host
IP_address_of_source_host
Shortname_of_destination_host
Shortname_of_destination_host
Shortname_of_destination_host
FQDN_of_destination_host
FQDN_of_destination_host
FQDN_of_destination_host
IP_address_of_destination_host
IP_address_of_destination_host
IP_address_of_destination_host
```

**Note**

EMC recommends that you resolve every name and IP address for each host three times to ensure that successive queries return correct and consistent values.

4. Use the **nslookup** command in interactive mode to validate reverse name resolution lookups in the reverse lookup zone with the Primary DNS Server:

- a. From a command prompt, type: **nslookup**.
- b. In the **nslookup** command prompt, type:

```
set q=ptr
```

- c. At the **nslookup** prompt, type:

```
IP_address_of_source_host
IP_address_of_destination_host
```

## Clearing the resolver cache

Each operating system uses a local resolver cache. A local resolver cache removes the reliance on checking name resolution services for each name resolution request, which increases the hostname resolution speed. The operating system checks the cache first to resolve the host, and if the host record exists, the operating system does not check other name resolution services. The operating system adds an entry to the resolver cache after the first successful hostname resolution, and the entry remains in the cache for a predetermined time.

On Windows only, to display the contents of the resolver cache, type the following command:

```
ipconfig /displaydns
```

Use the appropriate command to flush the contents of the resolver cache:

- On AIX and HP-UX:
  - For bind 9, type:

```
rndc flush
```

- For bind 8, type:

```
refresh -s named
```

- On Solaris and Linux, restart the `nscd` daemon.
- On Windows, type:

```
ipconfig /flushdns
```

## Verifying the NetWorker configuration

NetWorker contains two configurable options, the `servers` file that allows you to control access to a host and the `aliases` attribute in the Client resource, which allows you to define the names by which a host is known. When either option contains an incorrect host name, NetWorker operations can fail despite correct host name resolution and when an established connection exists between the source and destination hosts.

Ensure that the name that NetWorker uses primarily for a host appears consistently in all NetWorker resources. For example:

- Names of Client and Storage node resources.
- Names of the index database directory.
- Names specified in the Remote Access and Administrator attributes.
- Hostname references in resource attributes such as the Storage Node and Recover Storage Node attributes of a Client resource.
- Cached host certificates (NSR Peer information).

## Verifying the validity of the servers file

The `servers` file defines a list of remote hosts that can ask the local `nsrexecd` process to start a program. For example, the NetWorker server requests that the `nsrexecd` process on a client start the `save` process to begin a backup. The NetWorker installation process on certain operating systems prompts you to define remote hosts to add to the `servers` file. You can also manually modify the `servers` file at any time.

The `servers` file on a NetWorker host resides in the `res` subdirectory of the `nsr` directory. The location varies depending on the installation path.

When a host asks `nsrexecd` to start a process but the host does not appear in the `servers` file, a message similar to the following appears:

```
Cannot request command execution, permission denied
```

If you receive this message but the requesting host requires access, then manually edit the `servers` file on the destination host and add each short name and FQDN for the requesting host, on a separate line.

#### **NOTICE**

After you make changes to the `servers` file, stop and then restart the NetWorker services on the host. The *EMC NetWorker Security Configuration Guide* provides more information about how to modify the `servers` file.

## Confirming the validity of Aliases attribute

Each Client resource contains an `Aliases` attribute that defines a list of known names associated with the client. The NetWorker server generates this list the when you create the client resource.

You can also manually edit the `Aliases` attribute value to add or remove host name instances or IP addresses. Use the following guidelines when you modify the `Aliases` attribute value:

- Specify all short names and FQDNs for the host, including any retired host names.
- Specify each name on a separate line.

When the name returned by the operating system name lookup does not exist in any `Aliases` attribute for any client, a message similar to the following appears in the `daemon.raw` file:

```
hostname is not a registered client
```

## Clearing the NetWorker name cache

NetWorker maintains an internal name resolution cache that does not reflect any changes that you make to name resolution services until you restart the NetWorker services. When a NetWorker operation requires a name resolution lookup, NetWorker checks the internal cache first. If NetWorker finds the name in the internal cache, then NetWorker does not consult the operating system.

Use the `dbgcommand` command on the NetWorker server to send a list of cached names to the `daemon.raw` file:

```
dbgcommand -p nsrd_pid PrintDnsCache=1
```

where `nsrd_pid` is the process id of the `nsrd` process.

## Using multihomed systems

When the NetWorker server, storage node, or client has more than one IP address, you can specify the exact TCP/IP network path that NetWorker uses during a backup.

A multihomed system is a system that has any of the following types of NICs:

- More than one NIC, each having separate IP address.
- A single NIC with multiple IP addresses.
- Multiple NICs in a single bond that has multiple IP addresses.

## Multihomed system requirements

Before you configure NetWorker in a multihomed environment, review these requirements.

- Each IP address must always resolve to a unique primary hostname.
- Each IP address bound to a separate physical NIC must reside in a separate subnet.
- All the shortnames, FQDNs, and IP addresses for each NetWorker host must be correctly and consistently resolvable.
- Specify all of the hostnames that belong to a NetWorker server, storage node, or client in the Aliases attribute in the appropriate Client resource.
- Ensure that the `servers` file on each NetWorker client contains all the hostnames that resolve to the NetWorker server.

## Configuring multihomed hosts in a datazone

The following table summarizes how to configure the NetWorker environment to use a multihomed NetWorker server, storage node, and client.

**Table 112** Configuring multihomed hosts in NetWorker (continued)

| Multihomed host  | Required behavior                                                                                                                                                                                                                                                                    | NetWorker configuration requirements                                                                                                                                                                                                                                                                                                                                                                                                                                                             |
|------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| NetWorker server | The client sends metadata to the NetWorker server by using a specific NetWorker server NIC. The metadata includes the save set control session information and index database operations.                                                                                            | <p>The <code>servers</code> file on each client must contain the shortname and FQDN for each NetWorker server NIC.</p> <p>The Server network interface attribute of each Client resource must contain the FQDN of the NetWorker server NIC.</p> <p>Each instance of the Client resource must have the same value for the Server NetWorker Interface attribute.</p> <p>The Alias field for the NetWorker server Client resource must contain an entry for the shortname and FQDN of each NIC.</p> |
|                  | Each storage node device sends metadata to the NetWorker server by using a specific NetWorker server NIC. Metadata includes the device control session information and the media database operations that connect back to the <code>nsrmmdbd</code> process on the NetWorker server. | <p>The Server network interface attribute of each Storage Node resource must contain the FQDN of the NetWorker server NIC.</p> <p>The Aliases attribute of the NetWorker server Client resource must contain an entry for the shortname and FQDN of each NIC.</p>                                                                                                                                                                                                                                |

**Table 112** Configuring multihomed hosts in NetWorker (continued) (continued)

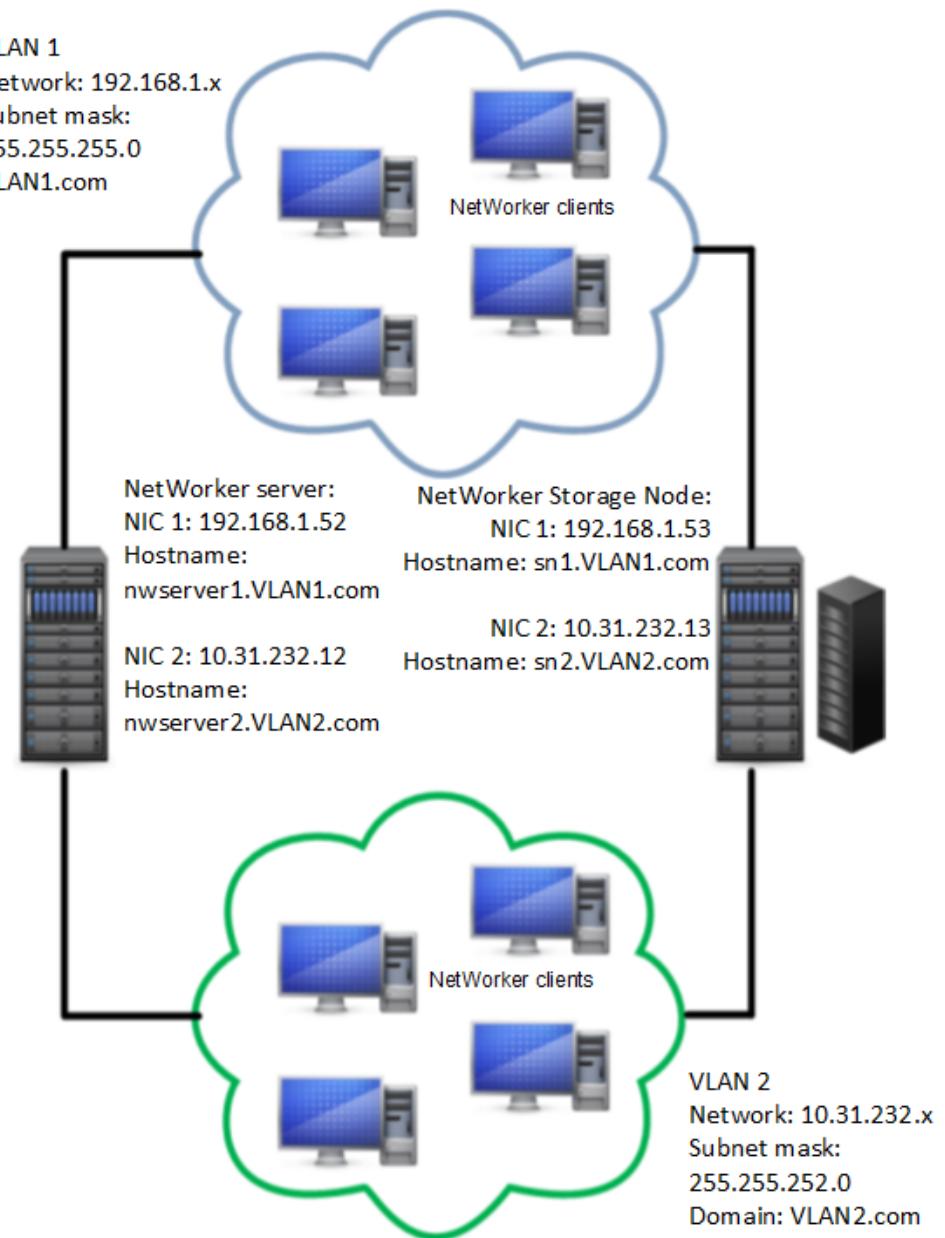
| Multihomed host | Required behavior                                                                                                                                                                                                                                       | NetWorker configuration requirements                                                                                                                                                                                                                                                              |
|-----------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|                 | Each storage node library sends metadata to the NetWorker server by using a specific NIC on the NetWorker server. The metadata includes SCSI commands for the tape movements and the library inventory operations that connect back to nsrmmgd process. | The Server network interface attribute of Library resource must contain the FQDN of the NetWorker server NIC. The Aliases attribute of the NetWorker server Client resource must contain an entry for the shortname and FQDN of each NIC.                                                         |
| Storage node    | The client sends backup data to a NetWorker storage node over a specific NIC.                                                                                                                                                                           | The Storage Nodes attribute of each Client resource must contain the FQDN of the storage node NIC. This also applies when the NetWork server is the storage node. The Aliases attribute in the Client resource for the storage node must contain an entry for the shortname and FQDN of each NIC. |
| Client          | The NetWorker server communicates with a client over a specific NIC.                                                                                                                                                                                    | When you create a Client instance for the client, specify a hostname for the client that is only reachable over the desired NIC.                                                                                                                                                                  |

## Configuring NetWorker in a multihomed environment

This section provides an example of how to configure NetWorker in a multihomed environment when the NetWorker server and the storage node have 2 NICs that

communicate through different networks. The following figure provides a graphical representation of the environment.

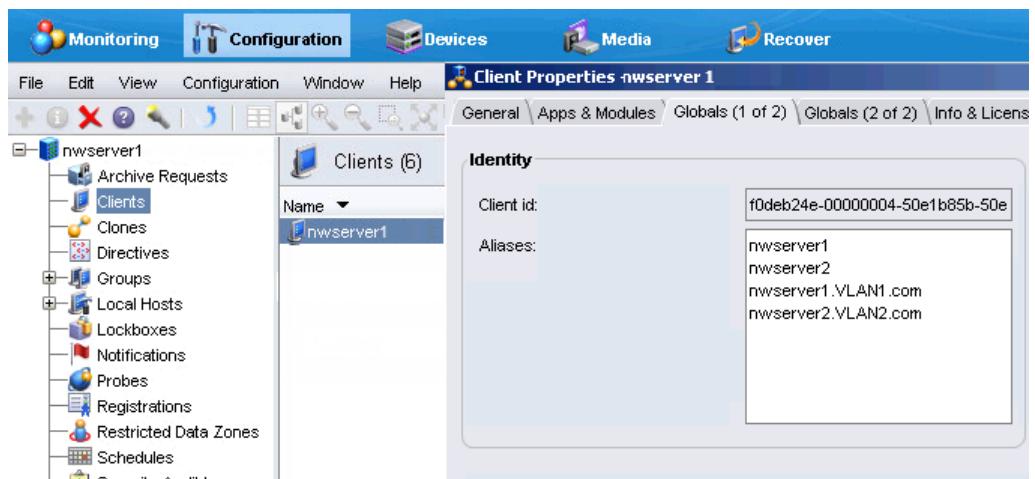
**Figure 40** Multihomed environment



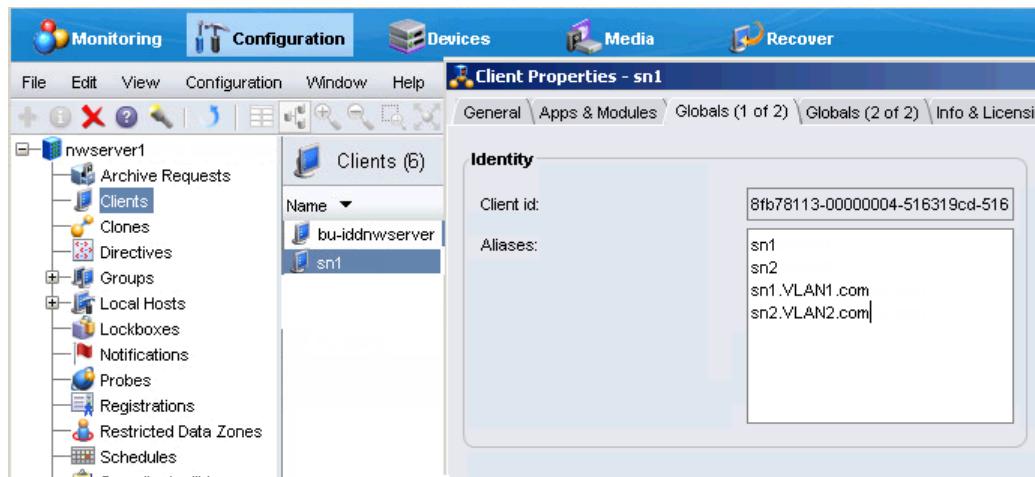
Complete the following steps to configure the multihomed environment:

#### Procedure

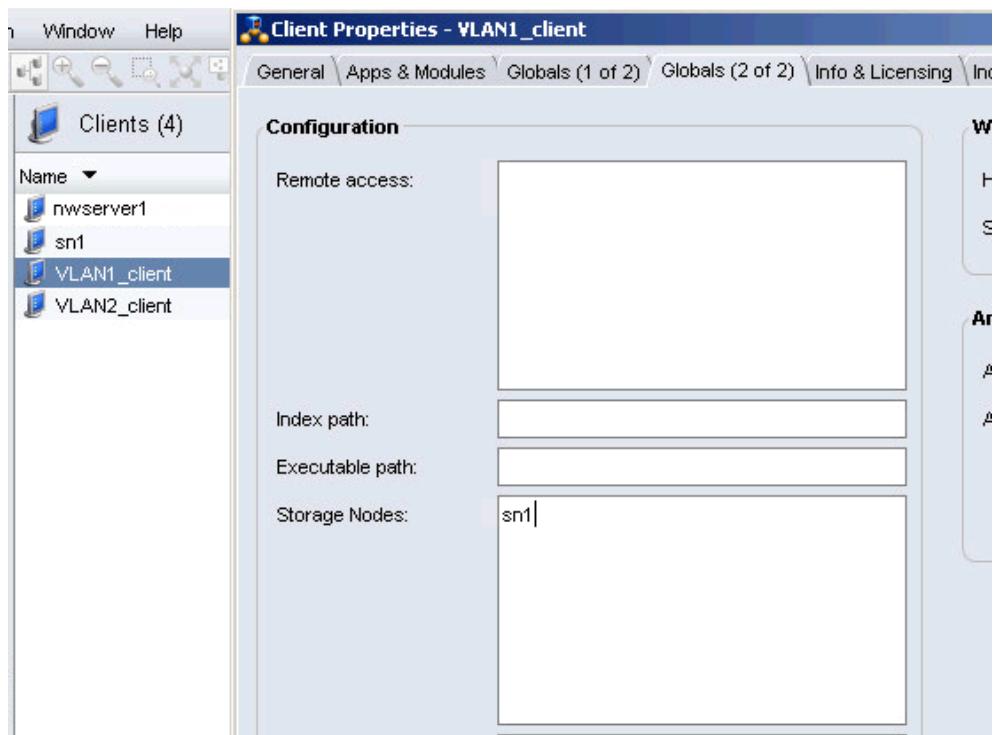
1. Update the **Aliases** attribute in the Client resource for the NetWorker server to include the FQDN and the shortname for each NetWorker server NIC. This figure shows the values in the Aliases attribute.

**Figure 41** Configuring the Aliases attribute for NetWorker server Client resource

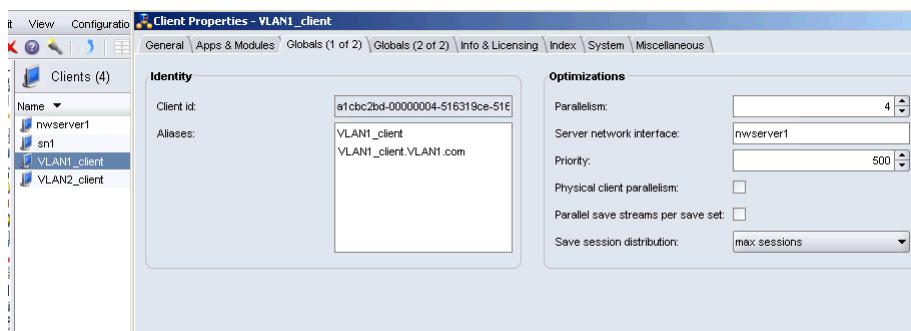
2. Create a Client resource for the storage node. Update the **Aliases** attribute to include the FQDN and the shortname for each storage node NIC. This figure shows the values in the Aliases attribute.

**Figure 42** Configuring the Aliases attribute for NetWorker storage node Client resource

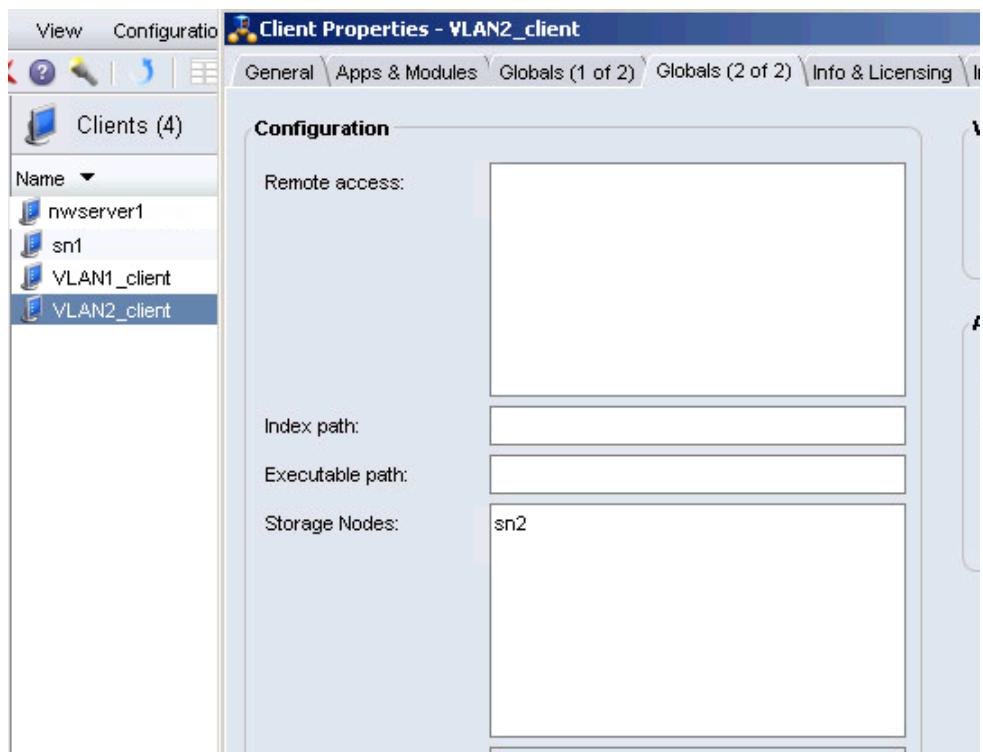
3. Update the **Storage Nodes** attribute for each Client resource in VLAN1 to contain the hostname of the NIC for the storage node to which the client connects. For example, for NetWorker client VLAN1\_client, specify the storage node hostname sn1. This figure shows the values in the Storage node attribute.

**Figure 43** Storage nodes attribute for clients in VLAN1

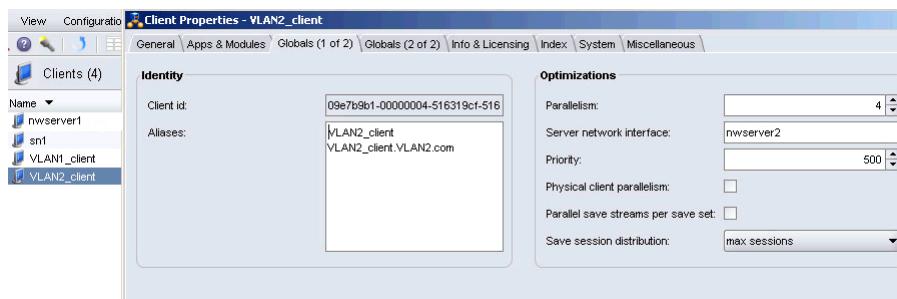
4. Update the **Aliases** attribute for each Client resource in VLAN1 to contain the FQDN and shortname of the client. The **Server network Interface** attribute must contain the hostname of the NIC for the NetWorker server to which the client connects. This figure shows the values in the Aliases and Server network interface attributes.

**Figure 44** Aliases and Server network interface attributes for VLAN1 clients

5. Update the **Storage Nodes** attribute for each Client resource in VLAN2 to contain the hostname of the NIC interface for the storage node to which the client connects. For example, for NetWorker client VLAN2\_client, specify the storage node hostname sn2. This figure shows the values in the Storage node attribute.

**Figure 45** Storage node attribute for clients in VLAN2

6. Update the **Aliases** attribute for each Client resource in VLAN2 to contain the FQDN and shortname of the client. The **Server network Interface** must contain the hostname of the NIC interface for the NetWorker server to which the client connects. This figure shows the values in the Aliases and Server network interface attributes.

**Figure 46** Aliases and Server network interface attributes for VLAN2 clients

7. Create the Device resource on the remote storage node by specifying either one of the hostnames for the storage node.

## NIC Teaming

NIC Teaming is a term that describes the use of multiple network interfaces in parallel. NIC teaming increases the link speed beyond the limits of any one cable or any one port and increases redundancy for higher availability.

Other terms for NIC Teaming include link aggregation, Ethernet trunk, port channel, port teaming, port trunking, link bundling, EtherChannel, Multi-Link Trunking (MLT), and NIC bonding.

NIC Teaming at the TCP level, regardless of the protocol or algorithm used, has no effect on a single TCP session. When you combine multiple links into a single link, the backup performance of a single session does not improve.

Depending on the algorithm used, starting parallel backup jobs with multiple NICs produces load balancing and can improve backup performance. To achieve load balancing, use a TCP session-based link aggregation algorithm and not a host-based algorithm. For example, use the IEEE 803.3ad/802.1ax Link Aggregation Control Protocol (LACP).

The use of trunked interfaces is transparent from a NetWorker point of view and the configuration of trunked interfaces inside NetWorker does not differ from the configuration of stand-alone interfaces. You can combine TCP trunking with multihoming, for example, by trunking some NICs on the system and leaving other NICs to work on separate subnets.

## Using DHCP clients

NetWorker relies on forward and reverse hostname and IP address resolution for communication between NetWorker hosts. When DHCP allocation changes an IP address, NetWorker cannot correctly resolve the current client IP address back to a valid hostname.

To back up DHCP clients, choose one of the following solutions:

- Configure the clients and the DNS Server to allow Dynamic DNS Registration. In this configuration, each time a client receives a new IP address, the DHCP service registers the hostname and IP address with the central DNS Server.
- Configure the DHCP server to always issue the same IP address to a host. In this configuration, bind the MAC address of the host to an IP address. Register this IP address in DNS Server or add the IP address to the `servers` file on the client and the NetWorker server.

**NOTICE**

EMC recommends that you do not configure the NetWorker server as a DHCP client. If the NetWorker server is a DHCP client, then the NetWorker server must use a reserved address that the DHCP server synchronizes with the DNS server.



# CHAPTER 27

## Troubleshooting

This chapter contains the following topics:

- [Before you contact technical support](#)..... 676
- [Viewing log files](#)..... 677
- [Locating savegroup job logs](#)..... 678
- [NetWorker functionality issues](#)..... 679
- [Devices and Autochangers](#)..... 690
- [NetWorker locale and code set support](#)..... 697
- [Enabling service mode for NetWorker](#)..... 697
- [Network and server communication errors](#)..... 697
- [NetWorker archiving and retrieval](#)..... 700
- [Storage nodes](#)..... 701
- [Console error messages and corrective actions](#)..... 703
- [NMC log files](#)..... 706
- [Console troubleshooting notes and tips](#)..... 707

## Before you contact technical support

If the solutions in this chapter do not solve the problem, go to the EMC online support web site for technical assistance.

Provide the following information.

- The software version of the NetWorker component.
- The operating system version.  
For example:
  - For Solaris, at the command prompt type the `uname -a` command.
  - For AIX, at the command prompt type the `oslevel` command.
- The hardware configuration.
- Information about devices and other SCSI IDs.  
To determine this information, use the following commands:
  - For AIX, Linux, and Solaris, enter the `/usr/sbin/inquire` command.
  - For HP-UX, enter the `/etc/ioscan` command.
- If you are using an autochanger, then the type of connection (SCSI or RS-232). Also, provide the version of the autochanger driver you are using:
  - For Solaris, enter the `pkginfo -x` command:  
`# pkginfo LGTOdrvrv`
  - For AIX, enter the `lslpp -l | grep EMC` command.
- Supply the following information:
  - How to reproduce the problem.
  - The exact error messages you encountered.
  - The number of times you have seen the problem.
  - If the NetWorker operation was successful before you made any changes and, if so, the changes you made.

## Determining the version of NetWorker software running on a client

To determine the version of the NetWorker software running on a client, use either the client properties window in NMC, the NetWorker User program on Windows or the `nsradmin` command.

### Determining the software version by using NMC

Use NMC to connect to the NetWorker server with a user that is a member of the Application Administrators user group on the NetWorker server.

1. On the **Configuration** window, select **Clients** from the left navigation pane.
2. Right-click the client and select **Modify client properties**.
3. On the **Info & Licensing** tab, review the **NetWorker version** attribute.

**NOTICE**

When you do not use the Client Configuration Wizard to create the client, NMC updates the NetWorker version attribute after the first backup. When you update the NetWorker software on a client, the NetWorker version attribute does not reflect the new version until the first backup after the update.

## Determining the software version by using NetWorker User

On Windows hosts, use the NetWorker User application to determine the NetWorker software version.

1. From the **Help** menu, select **About NetWorker User**. The NetWorker version number appears in the **About** dialog box.
2. Click **OK** to close the dialog box.

## Determining the client software version by using nsradmin

Use the nsradmin program on the NetWorker server to determine the version of the NetWorker software installed on a host, from a command prompt.

1. At the command prompt, type:

```
nsradmin -p nsrexecd
```

2. At the **nsradmin** command prompt, type:

```
nsradmin> show NetWorker version
nsradmin> print type: NSRLA
```

The nsradmin output displays the version of NetWorker software running on each client.

## Displaying diagnostic mode attributes

NetWorker resources such as clients and devices contain diagnostic attributes that are hidden by default from the Console server view.

1. Open the **Administration** window.
2. From the **View** menu, select **Diagnostic Mode**.
3. Right-click any resource and select **Properties** to see diagnostic attributes.

## Viewing log files

The `nsr_render_log` command renders internationalized NetWorker log files into the current locale of the host that the user uses to run the program. All other log files, as well as messages displayed in NMC, use the locale of the service that is generating the log message.

The `nsr_render_log` program is non-interactive. Use command line options to specify the log file that you want to view and the format of the output. The `nsr_render_log` program sends the results to `stdout`. You can redirect and save the output to a file.

The EMC NetWorker Security Configuration Guide describes how to perform the following log file operations:

- Render and view the log files manually with the `nsr_render_log` program.
- Render and view the log files manually from a remote machine, with the `nsr_render_log` program.

- Render the log files in the current locale at runtime
- Redirect the `nsr_render_log` output to a file

## Locating savegroup job logs

When you enable the Savegroup log by job id attribute on the NetWorker server resource, you can use the `jobsquery` command to locate logs for child jobs of a savegroup operation. This command takes a query, or query file, and searches the jobs database on the NetWorker server.

This example shows how you could use the `jobsquery` program to locate the child jobs of a savegroup job.

1. Open the `jobsquery` program and use the `show` option to specify which job attributes to display.

```
# jobquery
show type; command; completion status; start time; end time; job
id; parent job id; job log file
```

2. Use the `print` option to specify that only savegroup jobs will be displayed.

```
print type: savegroup job
```

The output shows that a savegroup with a job ID of 128000 completed successfully:

```
type: savegroup job;
command: ;
completion status: succeeded;
end time: 1228409390;
job id: 128008;
job log file: ;
parent job id: 0;
start time: 1228409364;
```

3. Use the `print` option to display all jobs whose parent job ID is 128008.

```
print parent job id: 128008
type: savefs job;
command: \
savefs -s daphne.lego.com -c daphne.lego.com -g Default -p -l full \
-R -v -F /usr/share/man/man1 /usr/share/man/man3;
completion status: succeeded;
end time: 1228409365;
job id: 128009;
job log file: /nsr/logs/sg/Default/128009;
parent job id: 128008;
start time: 1228409365;
type: index save job;
command: \
"save -s daphne.lego.com -S -g Default -LL -f - -m daphne.lego.com \
-V -l full -LL -W 78 -N
index:c177b9a2-00000004-4936d6d0-4936d6cf-0001c000-69\
7aa04f /nsr/index/daphne.lego.com";
completion status: succeeded;
end time: 1228409388;
job id: 128012;
job log file: /nsr/logs/sg/Default/128012;
parent job id: 128008;
start time: 1228409388;
```

Notice that the job log file attribute in the previous display shows the location of the job logs for two child job IDs: 128009 and 128012.

The *EMC NetWorker Command Reference Guide* or the UNIX man pages provide more information about the `jobsquery` command.

## NetWorker functionality issues

This section describes workarounds for NetWorker issues.

### Backup and recovery

This section covers backup and recovery operations.

#### Checking the NetWorker services

If you have trouble starting NetWorker programs, the services might not be running properly. On Windows systems, determine if these processes are running.

If they are not, start them:

- On Windows systems, go to **Control Panel > Administrative Tools > Services**.
- On UNIX systems, enter one of the following commands:

```
ps -ef | grep nsr
ps -ax | grep nsr
```

You should receive a output similar to the following

```
12217 ? S 0:09 /usr/sbin/nsr/nsrexecd -s jupiter
12221 ? S 2:23 /usr/sbin/nsr/nsrd
12230 ? S 0:00 /usr/sbin/nsr/nsrmmdbd
12231 ? S 0:01 /usr/sbin/nsr/nsrindexd
12232 ? S 0:00 /usr/sbin/nsr/nsrmmmd -n 1
12234 ? S 0:00 /usr/sbin/nsr/nsrmmmd -n 2
12410 pts/8 S 0:00 grep nsr
```

If the NetWorker daemons do not appear, start the NetWorker daemons.

#### Restarting a failed save set

Failed save sets can be restarted without requiring that the entire save group be re-run. You can initiate a restart from the `nsradmin` command line utility or from the `savegrp` program.

#### **NOTICE**

Bare Metal Recovery (BMR) enabled clients do not support the restart a single save set. This is because BMR workflows report all save sets within a save group as failure or success.

The following limitations apply to restarting individual save sets:

- Unable to accept requests if the restart window has passed.
- Unable to accept requests for clients with defined pre or post commands.
- Unable to accept requests if backup is in progress.
- Unable to restart a save set that completed successfully.
- Unable to restart a save set that is in progress.

## Commands that restart backups

You can use `nsradmin` or `savegrp` to restart failed save sets within a previously run save group.

### `nsradmin`

From the command line type:

```
# nsradmin
    nsradmin> . type: Nsr group; name: GroupName|Default
    nsradmin> update client subset: client1:ss1,ss2,
client2:ss3,ss4; autorestart: restart now
```

Output similar to the following appears:

```
update client subset: client1:ss1,ss2;client2:ss3,ss4; autorestart:
restart now
```

### `savegrp`

The `savegrp` program enables you to restart failed clients or save sets while a group is running. From the command line type:

```
savegrp -R -c "client1:ss1,ss2;client2:ss3,ss4" GroupName
```

### Note

When you use the `savegrp` program to restart individual save sets, `savegrp` does not accept requests during a bootstrap backup.

## Improper font size for the Client Wizard with Netscape on Solaris

When you use the Netscape browser on Solaris, the font size of the Client Wizard may appear too small.

To change the font type and size:

1. Open the `/usr/bin/nwwiz` script file in a text editor.
2. Edit the following line to change the font size:

```
NSR_WIZARD_FONT_SIZE=size
```

3. Save and close the `nwwiz` file.

## Backups fail to start when the daylight savings time change occurs

When you schedule backup operations to occur during the hour in which the operating system moves the clock ahead or behind by one hour, NetWorker skips the backup operation. For example, the operating system is configured to move the clock forward one hour at precisely 2:00 A.M. and backups are scheduled to occur at 2:01 A.M. At 2:00 A.M., the operating system moves the clock forward to 3:00 A.M. NetWorker will skip all backup operations that are scheduled to start between 2:01 to 2:59 and NetWorker does not initiate the backup operation.

To avoid this situation, set the backup time to occur at least one minute before the time change occurs.

---

**Note**

When you use the `mminfo` command to get a weekly save set usage summary for the time period during the change to daylight savings time, `mminfo` does not display any information for the day of the change.

---

## Shut down NetWorker services prior to any significant changes to system date

If you need to make a significant change to the system clock or date, for example, a change of more than a day, then ensure that you shutdown the NetWorker services before you make the change. NetWorker services depend heavily on the system clock for many operations such as active sessions, volume mount and unmount operations, the expiration of save sets, and license enforcement.

## Clone ID timestamp does not reflect the time the clone was created

To guarantee that the cloned save sets that NetWorker creates on different storage nodes do not have the same timestamp, the NetWorker software assigns a timestamp to cloned save sets that does not reflect the actual time that NetWorker creates the clone.

## Backups fail to stop

When you attempt to stop the backup process by clicking on Stop in the Group Control window all of the backup process for clients in the selected group should stop. However, the Stop action misses a client and messages appears, which indicates that the server is still busy.

To resolve the problem:

1. From the **Administration** window, click **Monitoring**.
2. Select the **Groups** tab and look at the messages that appear to determine which group are currently being backed up.

If the group status shows running `save` processes, but the associated `savegrp` process is not running, perform one of the following actions:

- Stop the conflicting group from running by clicking **Stop** in the Group Control window. [Stopping a group on page 434](#) provides more information.
- Shut down and restart the NetWorker services. [Stop and start a NetWorker server, client, or storage node on page 55](#) provides more information.

## Memory usage when browsing large save sets

When you use the NetWorker User program to browse or perform a browsable recover from a large save set, such as a save set with one million or more files, the operation may consume all of the memory on the host.

To avoid this issue, perform one of the following options:

- Perform a save set recovery. [Recovering the data on page 352](#) provides information about how to perform a save set recovery.
- Use the `recover` command, which enables you to directly browse the client file index and select the files and directories that you want to recover. Use this option to browse large save sets or when memory is limited on the host systems.

## Memory usage and nsrjobd

The `nsrjobd` daemon runs on the NetWorker server and is responsible for monitoring NetWorker activity during a backup or recovery operation. Depending on the size of your backup environment, `nsrjobd` can require large amounts of RAM.

## Media position errors encountered when auto media verify is enabled

To verify media, the `nsrmmd` process must reposition the volume to read previously written data.

The first attempt may not always succeed and the following warning messages appear in the message window of the NetWorker Administration window:

```
media warning: /dev/rmt2.1 moving: fsr 15: I/O error
media emergency: could not position jupiter.007 to file 44, record 16
```

If the server can find the correct position, media verification succeeds and a successful completion message appears:

```
media info: verification of volume "jupiter.007" valid 30052
succeeded.
```

If the media verification fails, then perform the following tasks:

- Reset the device.
- Verify the device configuration.
- Verify that NetWorker can recognize the media.
- Verify that the devic operations function properly.

## The scanner program marks a volume read-only

When you use the scanner program to rebuild the index of a backup volume, the scanner program marks the volume as read-only.

This is a safety feature that prevents NetWorker from overwriting the last save set on the backup volume.

Use the `nsrmm` command change the volume to write-enabled:

```
nsrmm -o notreadonly volume_name
```

## The scanner program requests an entry for record size

If you use the scanner program with the `-s` option but without an `-i` or `-m` option, a message similar to the following may appear:

```
Please enter record size for this volume ('q' to quit)
```

If this message appears, specify a block size that is greater than or equal to 32.

## Limitations for groups containing a bootstrap

NetWorker only writes bootstrap backups to a local device. When a group backup generates a bootstrap save set, ensure that device attached to the NetWorker server has an available volume for the bootstrap backup.

## Index recovery to a different location fails

If you attempt to recover indexes to a directory that differs from the original location, an error message similar to the following appears:

```
WARNING: The on-line index for client_name was NOT fully recovered.  
There may have been a media error. You can retry the recover, or  
attempt to recover another version of the index.
```

To resolve this issue, ensure that you recover indexes to the original location then move the indexes to another directory. [Moving a client file index on page 514](#) describes how to move indexes to another directory.

## Illegal characters in configurations

When you provide a name for label templates, directives, groups, policies, and schedules, do not use the following characters:

/ \ \* [ ] ( ) \$ ! ^ " ? ; ' ~ < > & | { }

## Error backing up large number of clients

When you use a Windows NetWorker server to back up a large number of clients, a CMD.exe application error windows may appear with a message similar to the following:

```
The application failed to initialize properly (0xc0000142). Click on  
OK to terminate the application.
```

If this problem occurs, edit the Windows registry on the NetWorker server to increase the desktop heap allocation.

1. In the **regedit32** application, navigate to the following registry entry:

```
HKEY_LOCAL_MACHINE\System\CurrentControlSet\Control\  
Session Manager\SubSystems\
```

2. Edit the **Windows** registry key.
3. Modify the third value of the **SharedSection** entry to increase the heap allocation size.

In the following example, the desktop heap allocation has been changed from a value of 512 KB to 1023 KB.

The original entry, with a desktop heap allocation of 512 KB appears as:

```
%SystemRoot%\system32\csrss.exe ObjectDirectory=\Windows  
SharedSection=1024,3072,512 Windows=On SubSystemType=Windows  
ServerDll=basesrv,1 ServerDll=winsrv:UserServerDllInitialization,3  
ServerDll=winsrv:ConServerDllInitialization,2 ProfileControl=Off  
MaxRequestThreads=16
```

The updated entry, with a desktop heap allocation of 1024 KB appears as:

```
%SystemRoot%\system32\csrss.exe ObjectDirectory=\Windows
SharedSection=1024,3072,1024 Windows=On SubSystemType=Windows
ServerDll=basesrv,1 ServerDll=winsrv:UserServerD1Initialization,3
ServerDll=winsrv:ConServerD1Initialization,2 ProfileControl=Off
MaxRequestThreads=16
```

4. Restart the NetWorker server.

The Microsoft Knowledge Base article 18480 on the Microsoft website provides more information.

## Hostname aliases

When you incorrectly define an alias for a client, the backup fails. Under certain conditions, such as improperly configured DNS servers or hosts files, the NetWorker software does not create any aliases for a new client. If you use TCP/IP, ensure that you specify the hostname and the fully qualified domain name (FQDN) for a client in Aliases field of the client properties window.

When the alias field is incorrectly defined you can see the following behavior:

- Backup operations for the client fail with the following error message:

```
No Client resource for client_name
```

- NetWorker always performs backups for a client at a level full, regardless of the level of the scheduled backup.
- Automatic index management, as set up in the browse and retention policies, does not work.
- The /nsr/index directory, which contains the indexes for all of the clients configured on the NetWorker server contains two directories for the same client, but each directory uses a different client name.

You will need to update the alias field for a client to include all hosts names for the client in the following situations:

- When a host have two or more network interfaces.
- When sites use a mixture of short and FQDNs for the same machines, for example, mars and mars.jupiter.com.
- When the data zone uses both (Network Information Services (NIS) and DNS).

### **NOTICE**

---

Do not include aliases shared by other hosts in the data zone.

## Directory pathname restrictions

A file manager (but not Windows Explorer) restriction causes errors when a pathname contains too many characters.

To avoid these errors, use a pathname that has fewer than 128 characters.

## Backup of a new client defaults to level full

The first time you back up a new client, a message similar to the following appears:

```
client: save: There are no save sets in the media database;
performing a full backup
```

This message indicates that NetWorker has not previously performed a back up of the specified save set. Before you can perform an incremental or level backup on a save set, perform a full backup of the save set.

If a level full backup exists for this save set, this error message can appear in the following situations:

- The clocks on the client and server are not synchronized.
- The savegrp session begins before midnight and ends after midnight.
- Multiple client ids exist for the client.

## Non-full backup of Solaris files with modified extended attributes

When you change the extended attributes for a Solaris file, but you do not modify the file, the action does not update the change time (ctime) for the file. As a result, the NetWorker software does not know that the extended attributes for the file have changed since the last incremental backup, and any non-full scheduled backup of the file system will not back up the file.

To ensure the file is backed up, use the `touch` command or otherwise modify the file so that the ctime is updated. Alternatively, perform a manual backup of the file. [Manual backups on page 71](#) provides more information.

## Client file index errors

This section provides information about issues are related to client file indexes.

### Renamed clients cannot recover old backups

The NetWorker server maintains a client file index for every client that has been backed up. When you change the name of the client, NetWorker uses the new hostname to create a new client file index, as a result you cannot recover files that were backed up under the old client name.

To recover data that was backed up by using the old client name, perform a directed recovery and specify the old client name as the source host and the new client name as the destination host. [Directed recoveries on page 348](#) provides information about how to perform directed recoveries.

### Missing client file indexes

Before you use the `scanner` program with the `-i` option, ensure that a client file index exists for the client associated with each save set. If you attempt to recover a client file index with the `scanner -i` command when the client file index does not exist, a message similar to the following appears:

```
scanner: File index error, file index is missing.  
Please contact your system administrator to recover or recreate the  
index.  
(severity 5, number 8)  
scanner: write failed, Broken pipe  
scanner: ssid 25312: scan complete  
scanner: ssid 25312: 91 KB, 13 file(s)  
scanner: done with file disk default.001
```

To resolve this issue, use the `nsrck -L2 clientname` to create a new client file index for the client, then try the `scanner` command again.

## Check failure of client file indexes

Each time the NetWorker server starts, the startup process uses an `nsrck -ML1` command to perform a level 1 consistency check on the client file indexes. In some circumstances, this consistency check does not detect corruption in the client file indexes. If you believe that the NetWorker server may have a corrupted client file index, run a higher level check on the index.

For example:

```
nsrck -L5
```

If the command does not resolve the index corruption, refer to [Recovering expired save sets on page 369](#) for more information.

## No notification of client file index size growth

The NetWorker server does not notify you when a client file index is getting too large. Monitor the system regularly to check the size of client file indexes. [Reduce the size of the client file index on page 516](#) provides information about how to manage the NetWorker client file indexes.

The *EMC NetWorker Command Reference Guide* or the UNIX man pages provide more information about how to use the `nsrls`, `nsrck`, and `nsrim` commands to monitor and manage client file indexes.

## Cannot use the Console interface to stop the `savegrp` command

If you start the `savegrp` command at the command prompt, you must stop the backup process from the command prompt.

If you attempt to stop the backup operation from the NMC Console window, a message similar to the following appears:

```
Only automatically started groups that are currently running can be stopped
```

## Aborting a recovery

When you stop a recovery operation on a client, the following could occur:

- The recovery might stop immediately.
- The recover program will display a list of the files that were not recovered.
- Messages similar to the following appears, which indicates that the recovery operation did not stop cleanly:

```
Recover: ***Cancelled***
Recover: Unable to read checksum from save stream
Recover: error recovering C:\WINDOWS\CURSORS\APPSTART.ANI
Didn't recover requested file C:\WINDOWS\CURSORS\APPSTART.ANI
```

## `xdr of win32 attributes failed for directory`

This error appears when the backup operation cannot back up the directory path. The rest of the save set completes successfully.

To resolve this problem, perform another backup of the directory.

## Cannot create directory *directory*

This error message appears when you attempt to relocate data to a directory that does not exist on the target host. You can ignore this message. The recovery process creates the new directory and completes successfully.

## The All save set and duplicate drive serial numbers

The All save set, which backs up all locally mounted drives and the VSS SYSTEM save sets, uses the serial numbers assigned to drives as part of the backup logic that determines when the backup operation should include a drive. If more than one local drive uses the same serial number, the All save set will only back up one of the drives.

To resolve this issue, perform one of the following solutions:

- Use the DiskProbe utility to set the serial numbers to unique numbers. The DiskProbe utility is part of the Windows Support Tools and is available for all versions of Windows supported by NetWorker software.
- Avoid using the All save set. Instead, specify each drive letter or the VSS SYSTEM save set separately. [Predefined save sets for scheduled backups on page 69](#) provides more information about the All save set.

## No disk label errors

This error message appears when you configure a non-optical device as an optical device.

To resolve this issue, verify that the Media Type attribute in the Device resource matches the expected media for the device, and correct if necessary.

## Cannot print bootstrap information

If the server bootstraps do not print, enter the name of the printer in the Group resource:

1. In the **Administration** window, right-click the group and select **Properties**.
2. On the **Setup** tab, in the **Printer** attribute specify the name of the printer.

## Server index not forced

If the NetWorker server belongs to a disabled group or does not belong to any group, the savegrp program does not back up the NetWorker server.

The information to recover server indexes is stored in the media database on the NetWorker server.

## Resolving copy violation errors

If you install the NetWorker server software on multiple hosts and more than one server uses the same NetWorker enabler code, a messages similar to the following appears in the save group completion email:

```
--- Unsuccessful Save Sets ---
* mars:/var save: error, copy violation - servers 'jupiter' and
  'pluto' have the same software enabler code, 'a1b2c3d4f5g6h7j8' (13)
* mars:/var save: cannot start a backup for /var with NSR server
  'jupiter'
* mars:index save: cannot start a backup for /usr/nsr/index/mars with
  NSR server 'jupiter'
```

```
* mars:index save: cannot start a backup for bootstrap with NSR
server 'jupiter'
* mars:index save: bootstrap save of server's index and volume
databases failed
```

To resolve this issue, perform one of the following actions:

- Remove the NetWorker server software from all hosts but one.
- Contact EMC Licensing and request new licenses for each additional NetWorker server.

#### Note

After you perform one of the resolutions, stop and then restart the NetWorker services on the NetWorker server that performs the backups.

## Converting sparse files to fully allocated files

The NetWorker server determines which files are sparse by comparing the allocated blocks with the byte size. If the allocated blocks do not account for the size of the file, NetWorker considers the file as sparse and the save operation replaces long strings of zeroes with “holes” in the recovered file.

A recovery operation may recover some files as sparse when the files were not sparse at the time of the backup operation. Oracle databases are susceptible to this problem because they are zero-filled, fully allocated files, but are not sparse.

To workaround this issue, use the `cp` command to copy the file after recovery:

```
cp recovered_filename zero_filled_filename
```

This command converts a sparse file to a fully allocated file.

#### NOTICE

Ensure that you have enough free disk space to accommodate a duplicate of each copied sparse file.

## Backing up large sparse files

To conserve backup media, NetWorker compresses sparse files before the save operation writes the file to the backup media. While NetWorker compresses the file, the backup job may stop and the following message appears:

```
savegrp: Aborting inactive job (633).
```

This can occur when the backup operation does not write any data to the backup media during the compression operation and time the backup is idle reaches the time specified by the group Inactivity Timeout attribute. To resolve this issue, increase the Inactivity Timeout attribute for the backup group.

To help determine an adequate timeout limit:

1. Set the **Inactivity Timeout** value to zero. A value of zero results in no timeout limit.
2. Determine the time the backup requires to complete a full save of the file system, and specify this time as the inactivity timeout limit. [Editing a group on page 249](#) describes how to set the Inactivity Timeout attribute for the group.

## Queries using the mmInfo -N command are case-sensitive

When you use the `mmInfo` command to query the media database, the `-N name` option is case-sensitive. The save set name the `-N` option references must match the case of the save set name that you specify in the save set attribute of the client resource.

However, when NetWorker performs a back up of drive partitions on Microsoft Windows (for example, C:\), the NetWorker server stores the save set name in uppercase in the media database.

For example, if the save set name that represents the drive partition was entered in the client resource is lowercase c, you must use uppercase C to query the media database:

```
mmInfo -N C:\
```

## Renamed directories and incremental backups

By default, if the name of a directory changes after a full backup, but no files or subfolders in the directory change, NetWorker will not include the renamed directory in subsequent incremental backups.

To include renamed directories in an incremental backup, select the `Backup renamed directories` attribute in the Client resource.

## Resolving names for multiple network interface cards

If any NetWorker host (client, storage node, server) has multiple network interface cards (NICs) with unique IPs and host names, you must configure all NICs and ensure that the host names are resolvable, even if the host does not use one or more of the NICs. Failure to have all NICs resolvable may cause problems with host connectivity to the NetWorker server.

Follow these steps to ensure that NetWorker uses the appropriate hostname for an IP address, and to ensure that you properly configure the hosts file and routing table on the host:

- Set up DNS to associate each IP address with a separate name.
- Configure the hosts file and routing table on each host that has multiple NICs with the appropriate IP address.
- Configure NetWorker to use the names that you configured in the DNS and hosts file.

## Configuring multiple NICs

In the following example, a dual-interface client connects to the NetWorker Server and Storage Node over `interface1` which has an IP address of 1.1.1.1 and has a dedicated connection to the Storage Node over `interface2` with an IP address of 2.2.2.1. The user wants to send all data to the Storage Node over `interface2` instead of the default `interface1`.

1. Configure DNS with unique host names for IP addresses 1.1.1.1 and 2.2.2.1. For example, `client-1` maps to 1.1.1.1 and `client-2` maps to 2.2.2.1. DNS should also be configured with unique host names for the IPs on the Storage Node. For example, `node-1` maps to 1.1.1.2 and `node-2` maps to 2.2.2.2.
2. Configure the routing table on the client to route the traffic through the correct interface, and then add the two IP addresses to the local hosts file.
3. On the NetWorker server, enter `node-2` in the Storage Node Affinity List of the client. [Configuring the client's storage node affinity list on page 127](#) provides more information.

The Networking chapter provides detailed information about configure a NetWorker data zone in a multi-homed environment.

## Libraries entering ready state

When you start the NetWorker service or after you configure a tape library, the library does not immediately enter the Ready state within NetWorker. This is normal behavior.

## Successful save sets listed as failed in the Group Backup Details window

Certain backup operations, such as the direct SCSI feature and some NetWorker modules, create multiple sessions to perform a single backup job. If one of these sessions fails, the Console will report that the entire backup job has failed.

To determine the status of each session, click the Show Messages button in the Failed table of the Savegroup Completion dialog. This information also appear in the Logs tab, under monitoring, and in the savegroup completion report.

## The NetWorker Server window does not appear on HP-UX

On HP-UX, the following error message appears after you log in to the NMC server and attempt to connect to a NetWorker server:

```
Unable to connect to server: Failed to contact using UDP ping
```

To resolve this issue:

1. In the NetWorker Console, select **Setup**.
2. Select **Setup > System Options**.
3. Unselect the **RPC ping via UDP when connecting to NetWorker** checkbox.

## Devices and Autochangers

This section explains how to resolve problems with devices and autochangers.

**NOTICE**

Do not edit device files and directories, this can result in unpredictable behavior and make it impossible to recover data.

## Additional attributes in the Autochanger resource

The Autochanger resource contains attributes that provide a detailed view of the hidden options that the `nsrjb` program uses. [Displaying diagnostic mode attributes on page 677](#) provides information about how to display hidden attributes.

The *EMC NetWorker Command Reference Guide* and the UNIX man pages provide information about these attributes.

**NOTICE**

Do not change time related attributes unless advised to do so by a Technical Support representative.

## Maintenance commands

NetWorker device driver software provides maintenance commands, such as `lusbinfo` and `lusdebug`, that you can use to diagnose problems on tape devices and autochangers.

The *EMC NetWorker Command Reference Guide* or the UNIX man pages provide information about how to use these commands.

## Autodetected SCSI jukebox option causes server to stop responding

If you use the `jbconfig` command to create an autodetected SCSI jukebox and the server stops responding, perform the following steps.

1. Start the `jbconfig` program
2. Select the option that installs an SII jukebox.
3. Enter the number that corresponds to the type of jukebox you are installing.
4. Proceed with `jbconfig` until this message appears:

```
Jukebox has been added successfully.
```

## Autochanger inventory problems

This section provides an overview of the situations that can result in an outdated autochanger inventory of volumes and how to update the inventory. When the jukebox inventory becomes outdated, the NetWorker software cannot use the autochanger.

The autochanger inventory can become out of date when:

- You manually eject the media from the autochanger drive.
- You manually remove the media is from the autochanger.
- You open the autochanger door.

To update the inventory and enable the NetWorker software to use the autochanger again, perform the following steps.

1. Verify that the volume is correctly installed in the autochanger and that the autochanger door is closed.
2. Log in as root or administrator on the NetWorker server.
3. Reset the autochanger:

```
nsrjb -Hv
```

4. Inventory: the autochanger:

```
nsrjb -Iv
```

The *EMC NetWorker Command Reference Guide* or the UNIX man pages provide complete details on the `nsrjb` command.

## Destination component full messages

When you perform a manual operation on an autochanger, for example when you use the buttons on the autochanger to unload the tape drive instead of unloading the tape drive by using NetWorker operations, a message similar to the following may appear:

```
Destination component full
```

To resolve the problem, use the `nsrjb -H` command to reset the autochanger.

## Tapes do not fill to capacity

The data stored on a tapes may not always fill the tape to capacity. For example, the NetWorker server can mark a tape with an advertised capacity of 4,000 MB full, after writing only 3,000 MB of data.

To enable NetWorker to use the maximum tape capacity, select the highest density device driver for the device. Additional reasons that the server appears to fill tapes prematurely include:

- Write errors occur during a backup. With any tape error, the NetWorker server marks the tape as full. To prevent tape write errors, clean the tape drive regularly and use only data-quality tapes. If cleaning the drive does not help, ensure that you perform the following actions:
  - Confirm the configuration of the device driver.
  - Set any necessary switch settings on the tape drive, based on the manufacturer specifications.
  - Confirm that all cables are secure.
  - Address other potential SCSI problems.
- Space requirements for NetWorker to create file marks. The NetWorker server periodically writes file marks to facilitate rapid recovery of data. These file marks consume varying amounts of tape space, depending on the type of tape drive. The number of file marks the server writes to the tape depends on how many save sets are on the tape. Many small save sets require more file marks than a few larger ones.
- Tape capacity differences. Two apparently identical tapes from the same vendor can vary significantly in capacity. This can cause problems when you copy one full tape to another, especially if the destination tape holds less data than the source tape.
- Data compression affects the tape capacity. If you use compression on the tape drive, you cannot predict the effect on tape capacity. A compressing drive can provide twice the capacity of a non-compressing drive. Tape capacity can vary depending on the type of backup data. For example, if a non-compressing drive writes 2 GB of data to a specific tape, the compressing drive could write 10 GB, 2 GB, 5 GB, or some other unpredictable amount of data.
- Tape length. Verify the tape lengths, for example, a 120-meter DAT tape holds more data than a 90-meter DAT tape.

## Tapes get stuck in drive when labeling tapes on Linux Red Hat platform

When you label a tape in a DDS configuration on a RHEL NetWorker server, the tape may become stuck in the drive and display the following error message:

```
unload failure-retrying 30 seconds
```

To resolve this issue, set the `auto_lock` setting attribute to “`0`” (Off) in the `/etc/stinit.def` file for the following drive types:

- Sony AIT-2 and AIT-3
- IBM LTO Gen1
- HP LTO Gen1
- IBM LTO GEN2

- IBM 3580 drive LTO-1
- IBM 3592 J1A
- Quantum DLT 7000

By default the `auto_lock` setting is set to 1 (On).

## Increasing the value of Save Mount Time-out for label operations

A label operation initiated by a backup operation may take more than 30 minutes before it fails when the Auto media management option is enabled and the label operation encounters a corrupted tape.

The NetWorker software keeps a record of the location of the corrupted tape only for the current backup operation, and NetWorker can attempt to use a corrupted tape for the other backup operation, unless an operator removes the volume.

To modify the time it takes the label operation timeout, modify the Save Mount Time-out attribute for the storage node. [Configuring timeouts for storage node remote devices on page 127](#) describes how to modify the attribute.

## Server cannot access autochanger control port

The control port controls the autochanger loading mechanism. The autochanger hardware installation manual contains information about how to verify that control port is properly connected.

If you cannot determine that the control port is working, contact the autochanger vendor for assistance.

### Modifying the control port

When a change in the control port of the robotic arm of a library occurs, NetWorker may not be able to perform library operations, such as labeling, mounting and unmounting, and inventorying. You may see the error `no such file or directory` when NetWorker attempts to perform library operations.

To update the NetWorker server or storage node to use the new control port, perform the following steps.

#### Procedure

1. Run the `inquire` command to determine the SCSI device address of the library arm and to confirm that a serial number is reported.

#### **NOTICE**

Use the `inquire` command with caution. The `inquire` command sends the SCSI inquiry command to all devices detected on the SCSI bus. If you use `inquire` during normal operations, unforeseen errors and possible data loss may result.

- If `inquire` reports the serial number of the arm, follow the procedure at [Scanning for libraries and devices on page 132](#) to scan the library for devices, then enable the library in NMC:
  - a. In the **Administration** window, click **Devices**.
  - b. Expand the **Libraries** folder, then right-click the library and select **Enabled/Disable**.
- If `inquire` does not report the serial number or if the scan for devices operation does not detect the control port change, use the `nsradmin` command to change the control port:

- a. Log in as root or as Windows administrator on the NetWorker host that manages the control port.
- b. At the command prompt, type **nsradmin**. The **nsradmin** prompt appears.
- c. To disable the library, type the following commands:

```
type: NSR jukebox
update enabled: no
```

- d. When **nsradmin** prompts you to update the resource, type **yes**.
- e. To update the control port, type:

```
update control port: scsiedev@b.t.1
```

where *b.t.1* is the bus.target.lun of the library's robotic arm (as reported by the **inquire** command).

- f. When **nsradmin** prompts you to update the resource, type **yes**.
  - g. To re-enable the library, type:
- ```
update enabled: yes
```
- h. When **nsradmin** prompts you to update the resource, type **yes**.
  - i. To verify that the control port was changed and the library is now enabled, type **print** at the **nsradmin** prompt.

## Changing the sleep times required for TZ89 drive types

When you unload a volume from a TZ89 tape device you may receive an error message similar to the following and NetWorker will repeatedly try to unload the tape:

```
nsrd: media info: unload retry for jukebox `COMPAQTL895' failed -
will retry again.
```

To resolve this issue, changes the sleep attributes in the Autochanger resource.

1. Shut down NetWorker services.
2. Shut down and restart the autochanger that contains the TZ89 drives.
3. When the autochanger is back online, restart NetWorker services. NetWorker will not attempt to unload the drive again.
4. Use NMC to edit the following autochanger sleep time attributes, and use the following values:
  - Eject Sleep: **18** secs
  - Unload Sleep: **40** secs
  - Load Sleep: **40** secs[Additional attributes in the Autochanger resource on page 690](#) provides information about how to set the sleep attributes.
5. Attempt to unload the drive again. If the drive fails to unload, repeat this procedure and increase the sleep times.

## Message displayed when CDI enabled on NDMP or file type device

If you enable the CDI feature for a NDMP tape device or file type device (FTD), a message similar to the following appears:

```
nsrd: media notice: The CDI attribute for device "/dev/rmt/3cbn" has
been changed to "Not used".
```

To avoid this message, do not enable the CDI attribute for these device types.

## Verify firmware for switches and routers

Ensure that the switches or routers firmware that you use on the network was manufactured after August 1995. Most of the switch and router vendors have significantly improved their handling of RPC traffic since August 1995.

## Commands issued with nsrjb on a multi-NIC host fail

When you run `nsrjb` commands to manage a jukebox on a NetWorker server or storage node that has multiple network interface cards (NIC), the commands may fail.

To prevent this failure, add the domain name of each additional NIC to the `Aliases` attribute in the Client resource for the NetWorker server or storage node. [Editing a client on page 528](#) describes how to edit a Client resource.

## SCSI reserve/release with dynamic drive sharing

When the NetWorker software uses Dynamic Drive Sharing (DDS) the operating system tape driver might use the SCSI reserve/release feature in a manner that interferes with the proper operations of the NetWorker software. To resolve this issue, disable the reserve/release feature.

### Solaris

The `st.conf` file contains a setting for each device type in use that enables or disables the SCSI reserve/release feature. The Tape Configuration section of the `st` man page provides more information. Use the most up-to-date `st` driver that is available for the version of Solaris.

Edit the `st.conf` file only if one of the following conditions apply:

- The NetWorker configuration includes DDS.
- Solaris `st` does not support a tape drive configured on a Solaris host.

To determine if the Solaris `st` tape driver supports a tape drive, perform the following steps:

1. Use the `mt` command to load a tape in the drive. For example, with the tape device file `0cbn`, the type: `mt -f /dev/rmt/0cbn status`
  - If the output of the `mt` command includes the line `SCSI tape drive` or appears similar to the following, the `st` tape driver uses generic settings, which do not support the tape drive:

```
mt -f /dev/rmt/4cbn status
Vendor 'IBM' Product 'ULT3580-TD2' tape drive:
sense key(0x6)= Unit Attention residual= 0
retries= 0 file no= 0 block no= 0
```

Tape operations may appear to work in NetWorker but you may run into problems when you attempt to recover saved data.

- If the output of the `mt` command appears similar to the following, the st tape driver recognizes the drive and uses the correct internal settings to manage the drive:

```
mt -f /dev/rmt/0cbn status
HP Ultrium LTO tape drive:
sense key(0x0)= No Additional Sense    residual= 0
retries= 0 file no= 0    block no= 0
```

In this configuration, you will only need to edit the `st.conf` file when you use the drive in a DDS configuration.

## AIX

To reset the reserve/release setting on an AIX operating system, use the SMIT interface.

1. From the **Devices** menu, select **Tapes**.
2. Change the value for the **RESERVE/RELEASE support** attribute from **No** to **Yes**.

## HP-UX

To reset the reserve/release setting on an HP-UX 11 operating system, perform the following steps.

1. Change the `st_ats_enable` kernel variable to a value other than zero.
2. (Optional) Restart the computer to ensure that the operating system implements the change.

---

### Note

The reserve/release is a fixed setting in HP-UX 10.

---

## Recovering save sets from a VTL on a different NetWorker server

The following procedure describes the steps that you need to perform before you can load a tape that was in a VTL managed by one NetWorker server into a different NetWorker server.

### Before you begin

Ensure the destination VTL is the same model, has the same drive names and the same number of drives as the original VTL.

### Procedure

1. Confirm the inventory of the VTL in the destination NetWorker storage node
2. Run the **inquire** command to determine the Control port of the VTL on the destination NetWorker storage node.
3. Run the **sjimm** command to load the tape into a drive on the destination NetWorker server.
4. Use the `mt` command to ensure that the tape status is online. For example: `mt -f device_name status`

When the `mt` command reports that the tape drive is online, you can use the `scanner` command to scan the save set information into the media database and client file index of the destination NetWorker server.

## NetWorker locale and code set support

The NetWorker software does not support locales defined by the operating system or code sets that remap characters, which have a special meaning for file systems. Depending on the file system, the special characters may include the slash (/), the backslash(\), the colon (:), or the period(.). De\_DE.646 is an example of one unsupported locale.

The NetWorker software might not function normally after you change the locale to an unsupported locale. Client file indexes that were created in a supported locale can become inaccessible.

## Enabling service mode for NetWorker

To enable and disable access to the NetWorker server, use the Accept new sessions and Accept new recover sessions attributes in NMC. When you unselect these attributes the server will not accept new backup and recovery sessions.

The *EMC NetWorker Security Configuration Guide* provides more information about these attributes.

When you restrict NetWorker server access, NetWorker takes all storage nodes offline, effectively putting NetWorker into a service mode operational state. In this state, you can stop any external client backup and recovery requests and prevent the start of scheduled group backups. Service mode provides you with a maintenance period where you can diagnose and troubleshoot issues before you return the server to normal operation.

You can also enable/disable specific storage nodes or devices to prevent use and allow for service operations. [Storage node configuration on page 124](#) describes how to enable/disable specific storage nodes. [Re-enabling a device on page 222](#) describes how to enable/disable a specific device.

## Network and server communication errors

This section provides general, UNIX and Windows network and communication issues that you may encounter in a NetWorker environment.

To help ensure successful communication between NetWorker clients and servers, each NetWorker host configured must not have any invalid or inactive IP addresses stored in the hostname resolution service (DNS, NIS, Active Directory, hosts file, and so on). Each IP address that maps to a host must have a configured network interface (NIC).

### Unapproved server error

If an unapproved server attempts to contact a client to initiate a backup, a message similar to the following appears: `client_name: server_name cannot request command execution.`

To provide additional servers access to the NetWorker client, perform the following steps:

1. Modify the `servers` file on the client and ensure that the file contains both the short name and the long name of the server. For example, the `servers` file on a NetWorker

client should contain these names for a NetWorker server named mars in the jupiter.com domain:

```
mars
mars.jupiter.com
```

2. In the **Alias** attribute of the Client resource, specify both the short name and the long name, and any other applicable aliases for the client.

## Unapproved server error during client setup

If you add a Windows client to a UNIX NetWorker server, and the servers file on a Windows client does not include the UNIX server host name, the message similar to the following may appear:

```
client_name: saveset_name Host server_name cannot request command
execution
client_name: saveset_name 10/13/00 11:48:26 nsrexec: Host server_name
cannot request command execution
client_name: saveset_name Permission denied
```

Ignore the message, and continue to add the client to the UNIX server. To avoid the message, add the UNIX server host name to the servers file on the client after you add the client to the UNIX server.

## Server copy violation

When the Alias attribute of the client resource for the NetWorker server does not contain all of the host names or aliases for the Networker server, the NetWorker server may become disabled and an error message similar to the following appears:

```
nsrd: registration info event: server is disabled copy violation
```

To resolve this issue, add all of the server aliases that are related to any additional network interfaces to the alias list of client resource for the NetWorker server.

## Remote recover access rights

You can control client recover access with attributes in the Client resource. The Remote Access attribute displays a list of the users that can recover save sets for a client. Add or remove user names depending on the level of security the files require.

---

### Note

If you enter a hostname or host=hostname in the Remote Access attribute, you allow any user on that host to recover files for the client. To enter a username without specifying the host, enter user=name.

The following users have permission to recover any files on any client, regardless of the users listed in the Remote Access attribute:

- ‘root’ user on a Unix host
- Member of the ‘Administrators’ local group on a MS Windows host
- Members of a ‘Application Administrator’ User group on the NetWorker Server
- Members of a NetWorker Server User group that has the ‘Change Security Settings’ privilege

Other users can only recover files for which they have read permission, based on file permissions at the time of backup. Files recovered by a user other than root, operator, or the operator group are owned by that user.

## Authentication fails due to duplicate host names

Authentication with the NetWorker server may fail if multiple NetWorker hosts share the same short name. For example, the data zone has two domains, accounting.company.com and marketing.company.com and each domain has a host named jupiter. The NetWorker server successfully authenticates jupiter.accounting.company.com. Authentication may fail when the jupiter.marketing.company.com attempts to contact the NetWorker server.

To enable the host to authenticate to the NetWorker server, perform the following steps.

1. On the NetWorker host that cannot authenticate with the NetWorker server, stop the NetWorker client service. [Stop and start a NetWorker server, client, or storage node on page 55](#) provides more information.
2. Delete the **nsrladb** database, which is located in NetWorker\_install\_path\res\lsrladb.

## NetWorker server takes a long time to restart

The consistency check of the media database, which occurs when the NetWorker server services start, can take a significant amount of time to complete when the media database is very large. While the NetWorker server performs the consistency check, client connections with the NetWorker server are delayed.

To reduce the size of the media management database, run the `nsrim -C` command when the NetWorker server is idle. Be aware that this command may take a long time to run and that the NetWorker server will be unavailable during this time. Run the command when the NetWorker server is not busy.

---

### Note

The `nsrim -C` command can take a long time to complete and you cannot perform NetWorker server operations until the command completes.

---

[Reduce the size of the media database size on page 516](#) provides more information about reducing the size of the media database.

## Changing the NetWorker server address

When the IP address changes on the NetWorker server, the NetWorker hostid also changes. The authorization code assigned to each NetWorker license depends on the hostid. When the hostid of the NetWorker server changes, you must contact EMC Licensing to generate new authorization codes based on the new hostid, then update each NetWorker license with the new authorization code.

If you do not re-register the software with the new authorization codes within 14 days of the hostid change, the NetWorker becomes disabled and you cannot perform any operations with the exception of recovery operations.

---

### Note

---

If you are using DHCP, use a static IP address for the NetWorker server.

## Binding to server errors

NetWorker architecture follows the client/server model, where the NetWorker servers use RPC to provide services to the client. These services reside in daemon processes.

When the daemons start, they register with the registration service provided by the portmapper.

If the NetWorker services are not running and an operation requests a NetWorker service, a messages similar to the following may appear in the savegroup completion email:

```
Server not available
RPC error, no remote program registered
```

These messages indicate that one or more NetWorker services are not running on the NetWorker server. The following table summarizes the startup commands that you can use to startup the services on a UNIX NetWorker server.

**Table 113** NetWorker Startup commands

Operating system	Startup command
Solaris, Linux	/etc/init.d/networker start
HP-UX	/sbin/init.d/networker start
AIX	/etc/rc.nsr

## New.Net and NetWorker software are incompatible

Software from New.Net, Inc. loads a dynamic link library (DLL) named newdotnet.dll, which modifies the Windows TCP/IP stack in ways that are incompatible with NetWorker software.

This causes many NetWorker programs, including save.exe, to fail on exit. This is a New.Net problem that the NetWorker software cannot work around. The Go!Zilla, BearShare, Mp3.com, iMesh, Babylon, Cydoor, Webshots, and gDivx products include the New.Net software. If you suspect that the New.Net DLL is the cause of problems, uninstall the New.Net software.

**NOTICE**

---

If you manually delete the newdotnet.dll file, the system will become unusable.

## NetWorker archiving and retrieval

This section explains how to troubleshoot issues with the Archive Module.

## Remote archive request from server fails

If a remote archive request from the NetWorker server fails, ensure that the username for the archive client (for example, root) appears in the Archive Users attribute of the Client resource for the archive client.

You can also grant NetWorker administrator privileges for root@client\_system in the Administrator attribute in the Server resource. However, be aware that NetWorker administrators can recover and retrieve data owned by other users on other clients.

## Multiple save sets appear as a single archive save set

When you combine multiple save sets in an archive, such as /home and /usr, NetWorker stores the archived data in a single archive save set. To retrieve archives separately, archive the save sets separately.

## Wrong archive pool is selected

If multiple archive pools exist in the NetWorker configuration, the archive operation will write the archive data to a volume in the last archive pool that was created on the NetWorker server .

## Second archive request does not execute

If you create two archive requests with the same name, NetWorker will only perform the first request.

To ensure that NetWorker performs all of the archive requests, do not create two archive requests with the same name.

## The nsrarchive program does not start immediately

If you run the nsrarchive command from a command-prompt, the archive operation does not start immediately. Wait a short time until the archive starts. Do not press [Ctrl]+[D] multiple times to stop the archive operation.

## Archive request succeeds but generates error when nsreexecd is not running

If the nsreexecd process is not running on a remote client during an archive request operation, NetWorker reports that the archive operations completed successfully, but the following error message appears in the daemon.raw file and the archive fails:

```
Failed to get port range from local nsreexecd: Service not available.
```

To resolve this issue, ensure that you start the nsreexecd daemon on a UNIX client or the NetWorker Remote Exec service on a Window client before you perform an archive operation.

## Storage nodes

This section provides troubleshooting information about storage nodes.

## Storage node affinity errors

A storage node affinity problem may exist when a backup fails with an error message similar to the following:

```
No matching devices; check storage nodes, devices or pools
```

This error message can appear for the following reasons:

- All of the devices in the storage node are disabled.
- Each device in the storage node contains a volume that does not match the pool that the backup request requires.
- All of the devices in the storage node are set to read-only.

To resolve this error:

- Enable devices on one of the storage nodes.
- Correct the pool restrictions for the devices listed in the Storage Nodes attribute of the Pool resource.
- Add another storage node that has enabled devices and meets the pool restrictions to the Storage Nodes attribute of the Pool resource.
- Write-enable one of the devices.
- Adjust the **Save Mount Timeout** and **Save Lockout** attributes for in the Device resource for the storage node.

## Storage node timeout errors

If the nsrd process starts on the NetWorker server and detects that a setting for the *NSR\_MMDCONTROL* variable exists, a message similar to the following appears:

```
NSR_MMDCONTROL env variable is being ignored  
use nsrmmmd control timeout attribute instead
```

If you receive this message, perform the following steps.

1. Shut down the NetWorker services.
2. Remove the environment variable setting for *NSR\_MMDCONTROL*.
3. Restart the NetWorker services.
4. Use NMC to connect to the NetWorker server.
5. Adjust the value of the **nsrmmmd Control Timeout** attribute in the Storage Node resource to the value that was assigned to the *NSR\_MMDCONTROL* variable, or to a value that best meets the current requirements. [Modifying the timeout attribute for storage node operations on page 126](#) provides more information.

## Console error messages and corrective actions

The following table provides a list of Console error messages or symptoms and corrective actions to take.

**Table 114** Error messages or symptoms

Error message or symptom	Possible cause	Corrective action
If the Console server fails to load and instead displays a Save As... dialog box.	JavaScript is not enabled on the host. The security level in Internet Explorer is set to High, which disables JavaScript, which is needed to launch the product), or JavaScript has been disabled by some other means.	In Internet Explorer, ensure that the security level is lower than high, which disables JavaScript, or enable Active Scripting.
The NetWorker server does not accept the authorization code.	A temporary enabler code has already expired.	Log out, then stop and restart the NMC server services.
An application window is unresponsive.	Insufficient disk space on the file system where the NMC database is installed.	<ul style="list-style-type: none"> <li>Ensure that the NMC server is running. <a href="#">Console troubleshooting notes and tips on page 707</a> provides details. If it is not, close all application windows and check the gstd log file for errors. <a href="#">Viewing log files on page 677</a> provides information about viewing log file.</li> <li>Back up and move the Console database, if necessary.</li> <li>On a Windows system, run InstallShield with the Repair option to move the database to a different drive.</li> </ul>
	Application ran out of memory.	Close all instances of the application and restart it.
	Another dialog box is open in the NMC window or Administration window.	Close any open dialog boxes or error messages.
Connection refused: no further information. or Problem contacting server server_name:	NMC server is in the process of crashing or has already crashed.	<p>Check to see if the NMC server is running.</p> <ul style="list-style-type: none"> <li>If it is running, stop and restart the NMC server.</li> <li>If it is not, close all application windows and check the gstd log file for errors. <a href="#">Viewing log files on page 677</a> provides information about viewing log files.</li> </ul>

**Table 114** Error messages or symptoms (continued)

Error message or symptom	Possible cause	Corrective action
	Console server has been started within the previous few minutes.	Wait a couple of minutes and retry.
Failed to bind to port <i>port_number</i> message appears in the <i>gstd.raw</i> log file.	Another process is using the <i>gstd</i> service port (default 9001) or the port is in a timeout (TIME_WAIT/FIN_WAIT) state.	Close any running NMC GUIs or any processes that may be using the <i>gstd</i> service port. Wait until the timeout period passes so that the operating system can free up the port. The timeout period may differ between operating systems.
Database fetch operation failed messages appears in the <i>gstd.raw</i> log file.	The NMC database is corrupt.	Recover the database. <a href="#">Recovering the NMC server database on page 387</a> provides details.
Display problem: In Internet Explorer:  The page cannot be displayed.	The <i>gstd</i> service is not running on the NMC server.	Restart the NMC server.
	Browser is not pointing to the correct URL.	Check the install log file to determine the HTTP port used by the NMC server. <a href="#">The install log on page 707</a> provides details.
	Network connection is down.	Ping the NMC server to confirm the network connection. If it is available, contact the system administrator.
Enabler code not accepted.	Temporary enabler code has expired.	Close the Console server and log in again. Repeat the procedure of entering the enabler code. If the enabler code is still not accepted, log out, then stop and restart the Console server.
Database delete operation failed: Reference object does not exist.	Another user has already deleted that user or folder.	None
Database store operation failed: An object with pathname “ <i>pathname</i> ” already exists.	<ul style="list-style-type: none"> <li>• Another user is trying to add a folder to the same location in the Enterprise at the same time.</li> <li>• An object was added with the same name as an existing object.</li> </ul>	<ul style="list-style-type: none"> <li>• Wait a few moments and try again.</li> <li>• Check whether there is an existing object with the same name.</li> </ul>
Invalid Object ID.	Another user deleted that host.	None

**Table 114** Error messages or symptoms (continued)

Error message or symptom	Possible cause	Corrective action
Could not contact License Manager on <i>hostname</i> . - or - Program not registered.	License Manager hostname has not been assigned or License Manager is not running or installed.	If you are using the License Manager and a hostname has not been assigned: Select the Software Administration task. Click Licensing.  Click Software Administration on the menu bar.  Click Change LLM Server.  Enter the new License Manager hostname.  Click OK.  If License Manager is installed, but not running, start it.  The <i>NetWorker License Manager Installation and Administrator's Guide</i> provides details.
	NetWorker client was stopped, but the License Manager was not stopped, and then the NetWorker client was restarted.  Although both services are now running, NetWorker client must be started <i>before</i> License Manager is started. If the services are not started in the correct order, an error condition occurs.	Stop the NetWorker software. Stop License Manager if it is running. Restart License Manager.  Restart the NetWorker software.
License allocation failed.	Temporary license for NetWorker software is expired.	Enter enabler codes and register the product.
License managed event indicates that license is expiring/expired even though it has been authorized.	License has been authorized within the last 24 hours.	None needed. To remove the managed event from the display, dismiss the event or it will be deleted within 24 hours.
Logging of debug messages has stopped. alloc /opt: file system full.	Disk space on the /opt file system is nearly full.	Allocate more disk space.
Event disappears from the Events window.	Another user dismissed it, or the problem that was causing the event no longer exists.	None

**Table 114** Error messages or symptoms (continued)

Error message or symptom	Possible cause	Corrective action
Dialog box: "Java Web Start –Download Error" with the message, "Unable to launch NetWorker Console".	Java Web Start preferences are set to something that is incompatible with the rest of the environment. (For example, a proxy server has been set up that stops Java Web Start from downloading the Console client software from the Console web server.)  This error message may also occur if the Console is being launched on a localized operating system and the Java Web Start cache path contains non-English characters.	Check the Preference settings in the Java Web Start Application Manager for compatibility with the environment. Change any settings that prohibit the download of the Console client software.  In the proxy server example, go to the General tab of the Preferences dialog box and select None, for Proxies.  If the Java Web Start cache path contains non-English characters, change the path to contain no non-English characters.
gstd.log file error: internal error: could not end transaction	When you move the system time ahead, the NMC server initiates a time out event and closes database client connection for the gstd process.	None

## NMC log files

By default, the `/opt/lgtonmc/logs` directory on UNIX or `C:\Program Files\EMC NetWorker\Management\GST\logs` folder on Windows contains the NMC log files.

The NMC server produces the following log files:

- `install.log`
- `gstd.raw`
- `db_output.log`
- `dbstop_output.log`
- `dbstop_output.log`
- `web_output`

## The install log

The install log files contains information that can help you troubleshooting a problem with the NMC server and to tracking decisions that were made during installation process. For example, which HTTP service port was specified to access the web interface.

## The gstd log

The `gstd.raw` file contains the messages for the NMC server.

[Viewing log files on page 677](#) provides information about viewing log files.

Each time the NMC server starts, the `gstd` process checks the size of the `gstd` log file. If the `gstd` log file has reached the maximum size defined by the NMC configuration, the NMC server creates a new `gstd.raw` file. The following table provides an example of the variables that you can configure to control the `gstd.raw` file.

**Table 115** Environment variables for the `gstd.raw`

Variable name	Description
<code>GST_MAXLOGSIZE</code>	Sets the maximum size of the <code>gstd</code> log file before it is renamed on GST restart.
<code>GST_MAXLOGVERS</code>	Sets the maximum value of <code>nnn</code> in <code>gstd.nnn</code> .
<code>GST_DEBUG</code>	Sets the level of verbosity of the <code>gstd</code> log file. Can also be set from the System Options dialog box.

[Setting system options to improve NMC server performance on page 470](#) provides more information about all of the environment variables available to configure the NMC server.

## Console troubleshooting notes and tips

This section provides general troubleshooting tips for the NMC server.

### Troubleshooting an NMC server that is not responding

If the NMC server is not responding, answer the following questions:

- Is a potentially long-running process such as a device operation (label or inventory, for example) currently running?  
Any process that you start on the Console server locks the user interface until that process completes. To perform multiple, long-running operations simultaneously (that is, to administer multiple NetWorker servers), open a separate web browser instance of the NMC server to run each operation.
- Are the all of the following processes running?
  - GST server (`gstd`)
  - Database server `dbsrv12`
  - Web server (`httpd`)
- Is the `ntpdate` command synchronizing at midnight?  
In some cases, when you have a cron job that perform an `ntpdate` synchronization at exactly midnight, the NMC server may lose connection to the database. To resolve

this issue, modify the time that the cron job performs the ntpdate synchronization or have ntp run as a service and synchronize continuously.

## Determining if the Console server is running on a Windows system

On a Windows computer:

1. From the **Start** menu, select **Control Panel > Administrative Tools > Services**.
2. Verify that **EMC GST Service** is running.

## Determining if the Console server is running on a Solaris system

Use the `ps` command to confirm that the process, which the NMC server requires are running

- For the `gst` server process, type:

```
/usr/bin/ps -ef | grep gstd
```

If the `gstd` process is running, output similar to the following appears:

```
root      6140      1      0 12:54:10 ? 0:03 /opt/lgtonmc/bin/gstd
```

- For the database server process, type:

```
/usr/bin/ps -ef | grep dbsrv
```

If the database server is running, output similar to the following appears:

```
LGTOMC root      6140      1      0 12:54:10 ? 0:03 /opt/lgtonmc/sybasa/bin/dbsrv12
```

- For the web server process, type:

```
/usr/bin/ps -ef | grep httpd
```

If the web process is running, output similar to the following appears:

```
LGTOMC root      6140      1      0 12:54:10 ? 0:03 /opt/lgtonmc/bin/httpd
```

## Unable to connect to host: Please check Security setting and daemon logs on the Networker client and Console server for more details

This message can appear when you perform Client Configuration wizard tasks, Device Configuration wizard tasks, or when you browse save sets at the same time that you add or modify a client resource.

Check for one of the following scenarios when you receive this error.

- Verify that the SSL key matches between the NMC Server and the NetWorker client host. The SSL key is in the NSR Peer Information attribute, which is located in each host's nsrladb database. A mismatch can occur when the nsrladb on one host is corrupted.

To resolve this issue, delete the Console Server's NSR Peer Information from the NetWorker Client's nsrladb, and delete the NetWorker Client's NSR Peer Information from the Console Server's nsrladb as following:

- To delete the Console Server's NSR Peer Information from the NetWorker Client's nsrladb, on the client host, type:

```
nsradmin -p nsrexec
nsradmin> print type:NSR peer information
```

---

**Note**

Identify the Console Server's NSR Peer Information, and delete it.

```
nsradmin> delete type: NSR peer information;name:<Console Server name>
Delete? Yes
```

- To delete the NetWorker Client's NSR Peer Information from the Console Server's nsrladb, on the Console Server host, type:

```
nsradmin -p nsrexec
nsradmin> print type:NSR peer information
```

---

**Note**

Identify the NetWorker Client's NSR Peer Information, and delete it.

```
nsradmin> delete type: NSR peer information;name:<Client name>
Delete? Yes
```

After the deletion is complete, it is not mandatory to restart the NetWorker or Console services.

- The Client cannot resolve hostname of NMC Server or NW Server. Sometimes, NMC can resolve the client hostname, but, client cannot resolve NMC or NetWorker Server hostname.  
To resolve this issue, ping the NetWorker Server and NMC server from the Client. If the ping fails, DNS is not resolving the hostname issue and add the hostname to the client hosts file.
- Ensure NetWorker users have at least the “Operate NetWorker” privilege to launch the Client Wizard. To resolve this issue, add the user to the appropriate user\_group in the NetWorker Server.
- The NetWorker Server may not be present in the client's servers file. To resolve this issue, add the NetWorker Server to the client's servers file.
- The NMC Server, NetWorker Server and NetWorker client hosts must only use nsrauth authentication.

## Username/password validation fails when you use the NMC New Device wizard to configure an AFTD if storage node is UNIX

When you use the NMC New Device Wizard to configure an AFTD, the username/password validation for browsing the file system may fail for a UNIX storage node .

This failure can occur in the following situations:

- The system is missing the Pluggable Authentication Modules (PAM) library.
- The rule in the pam.conf file (/etc/pam.conf) for OTHER service is set to deny.

The operating system documentation provides more information about how to install the PAM library and how to modify the pam.conf file.

## Querying large numbers of save sets in the NetWorker user interface may cause a Java heap space error

When you query a large numbers of save sets in the NetWorker user interface, the query may fail with a Java heap space error.

To resolve this issue, increase the Java heap size that the NMC application uses.

1. On the NMC server host, open the *Console\_install\_dir\web\gconsole.jnlp* file in a text editor.
2. Increase the *default max-heap-size* value from 700MB to 1400MB.

For example:

```
<resources>
<j2se version="1.5+" initial-heap-size="64M"
max-heap-size="1400M"/>
```

---

### Note

To provide meaningful query results and to reduce the chance of encountering this error, narrow the save set search criteria by specifying selection parameters.

---

## NMC user interface exits unexpectedly

If the NMC GUI loses its connection to the gstd service because the gstd service was shutdown or failed, then the GUI displays a warning and exit after 10 seconds. This is normal behavior. [Console error messages and corrective actions on page 703](#) provides more troubleshooting information.

# APPENDIX A

## Backing Up and Restoring a Microsoft DFS

This appendix contains the following topics:

- [Overview of a Microsoft DFS](#)..... 712
- [DFS topology information](#)..... 713

## Overview of a Microsoft DFS

Microsoft DFS is a Windows file system feature that enables you to create a namespace of shared directories that are physically distributed across a network. With DFS, you can organize a set of distributed directories logically, according to any scheme you choose, to provide centralized access to files that reside in a variety of locations.

Benefits of DFS include:

- Easy browsing of servers
- Simplified searches for files and data
- Server load balancing

### Domain-based DFS

Domain-based DFS has the DFS topology information stored in Active Directory (AD). Because this information is replicated on multiple domain controllers, domain-based DFS is fault tolerant. The DFS host server can be any Windows domain controller or member server.

### Registry-based DFS

Registry-based DFS, also called stand-alone DFS, has the DFS topology information stored in the Windows registry on the DFS host server.

### DFSR

DFS Replication (DFSR) provides basic file replication between servers. DFSR identifies modified or new files, and copies only those parts of files that have changed or been added.

### DFS junctions

A DFS junction is a DFS root or link.

- A DFS root is a namespace for files and DFS links.
- A DFS link is a connection to a shared file or folder.

DFS junctions are file system objects, not files or directories. Therefore, the NetWorker software does not treat DFS junctions the same as files or directories for backup and recovery. However, DFS junctions appear as files and directories in the NetWorker User program.

### Save Set ALL-DFSR

NetWorker has a save set type called All-DFSR which includes all DFS related save sets for a specified backup. Unlike other all-inclusive save set types, ALL-DFSR is not related to any particular file system. ALL-DFSR backs up all components defined by DFS\FRS writers.

The syntax for this save set is ALL-DFSR. It is not case sensitive. ALL-DFSR does not support BBB. BBB only creates backups at the volume level and DFSR replication folders can be a subfolder, which creates a conflict. Synthetic full backup is not supported with ALL-DFSR. If ALL-DFSR is specified for a system where DFS or FRS is not installed, backup will fail.

The ALL-DFSR save set registers the corresponding writer and writer component nodes under WINDOWS ROLES AND FEATURES. All Replication folders are restored through these nodes.

## DFS topology information

Domain-based DFS topology information is backed up as part of AD, which is a component of the Windows Roles and Features save set on domain controllers. Registry-based DFS topology information is backed up as part of the Windows registry, which is a component of the DFS host server's Windows Roles and Features save set.

## Configuring a scheduled DFS backup

To avoid inconsistencies among the various save sets, configure a scheduled backup that includes the DFS topology information, junctions, and destination directories. Alternatively, you can use the ALL-DFSR save set.

### NOTICE

When a DFS client resource is run for the first time, the save set sizes should be verified to ensure that they are correct.

---

To configure a scheduled backup for a DFS:

### Procedure

1. In the **Administration** screen, include the following clients in the NetWorker group that will back up the DFS:

- The DFS host server
- Any computer where remote DFS destination directories reside
- A domain controller (domain-based DFS only)

For example, you could create a NetWorker group named DFS, then make each of the preceding clients a member of the DFS group. The topic, *Backing up data*, provides more information about configuring a scheduled backup.

2. Enter the following save sets in the **Save Set** attribute of the DFS host server's client resource:

- The DFS root. For example:

C:\MyDfsRoot

- DFS destination directories that reside on the DFS host. For example:

D:\MyLocalDir

---

### Note

DFS destination directories are also be backed up if you enter the entire volume (for example, D:\) in the Save Set attribute.

3. For clients where remote DFS destination directories reside, enter the destination directory paths in the **Save Set** attribute. For example:

```
E:\MyRemoteDir
```

```
E:\MyOtherRemoteDir
```

```
E:\
```

## Restoring a DFS

Restore DFSR through Windows Roles & Features.

### Procedure

1. Restore the DFS topology information:
  - To restore a domain-based system, restore the Windows Roles and Features save sets on the domain controller.
2. On the DFS host server:
  - a. Restore the DFS root.

---

**Note**

You cannot restore individual DFS links. If the DFS root has lost a link, restore the entire DFS root in which that link resided.

---
  - b. If necessary, restore any local DFS destination directories.
3. If necessary, restore the remote DFS destination directories.

## Authoritative restores of DFS Replication writers

You must perform authoritative restores of the DFS Replication writers from the command line. Restores from the NetWorker User program GUI are not authoritative.

To perform an authoritative restore of the DFS Replication writer, use the **-U** option with the *recover* command.

The following examples assume that you have two DFSR shares, `E:\Share1` and `E:\Share2`.

- To restore all the DFSR shares (two shares in this example), type the following command:

```
recover -s server -U -N "WINDOWS ROLES AND FEATURES:\DFS  
Replication service writer"
```

- To restore just one DFSR share (Share1 in this example), type the following command:

```
recover -s server -U -N "WINDOWS ROLES AND FEATURES:\DFS  
Replication service writer:Share1"
```

## Non-authoritative DFS Replication writer granular recovery

Windows Distributed File System Replication (DFSR) granular recovery is supported on Windows Server 2008, Windows Server 2008 R2, Windows Server 2012 and Windows Server 2012 R2.

DFSR Shared Directories supports granular DFSR folder and file recoveries on computers that run Windows Server 2008 and later operating systems. You do not have to recover

the entire Windows Roles and Features save sets to restore DFSR shared directories. If you perform a file level non-VSS granular recovery, then the recovered file is treated as new version of the file by DFS.

You must use volume backup to correctly back up a DFSR namespace. Also, namespaces are skipped when specifying the All save set. You must back up namespaces directly by specifying the path of the namespaces as separate save sets in the Save Set attribute.

For recovery of namespace data, use the NetWorker User program and select individual files or folders of the NetWorker client resource.



## APPENDIX B

# Additional Features of the Microsoft Windows Server

This appendix contains the following topics:

- [NetWorker Module for Microsoft](#).....718
- [Active Directory](#).....718
- [Encrypting file system](#).....718
- [Event logs](#).....719
- [Internet Information Server](#).....719
- [Windows registry](#).....720
- [Sparse files](#).....720
- [Advanced Configuration and Power Interface](#).....720
- [Windows print queues](#).....720
- [Windows Optimized Deduplication](#).....721

## NetWorker Module for Microsoft

NetWorker Module for Microsoft (NMM) provides VSS-based backup and recovery of the Windows operating system, and Microsoft server applications, for example Microsoft Exchange Server, Microsoft SQL Server, and Microsoft SharePoint Services.

The *EMC NetWorker Module for Microsoft Administration Guide* provides more information about the NMM product.

## Active Directory

Active Directory (AD) is the Windows directory service and the foundation for the Windows Distributed File System. AD is a component of the Windows system state on Windows Server domain controllers. A domain controller is a computer that stores directory data and manages user interactions with a domain, including login, authentication, directory searches, and access to other shared resources.

### Active Directory backups

The NetWorker software automatically backs up AD as a component of the the WINDOWS ROLES AND FEATURES save sets, which are included in a Windows BMR backup . An AD backup or restore includes the AD log files, database, patch files, and expiry token.

### Active Directory recoveries

The *NetWorker Procedure Generator* contains information about the online recovery of Active Directory. [Windows Bare Metal Recovery on page 611](#) provides information about the bare metal recovery of an Active Directory host.

## Encrypting file system

Windows Encrypting File System (EFS) allows NTFS files to be stored in encrypted format. A user without the private key to the file cannot access the file.

Consider these when backing up or recovering files or folders that are encrypted with EFS:

- NetWorker software will not encrypt or compress a file already encrypted by Windows.
- Do not use AES encryption when backing up files that are encrypted using EFS.
- Files can become unusable if the encryption keys change on the domain controller. Reasons include:
  - The domain controller functionality is moved from one computer to another
  - The domain controller crashes.
- NetWorker software does not back up encryption keys. If the EFS is reinstalled after a disaster, the new security keys will not match the recovered keys and the recovery will fail. Keep a copy of the keys to ensure a successful recovery.
- You cannot perform a directed recovery of encrypted files.
- When recovering encrypted files to an encrypted folder that has been removed, consider the following:
  - If you recover the encrypted files and the encrypted folder, the recovered folder and files are all encrypted.

- If you recover only individual encrypted files (but do not recover the encrypted folder that contains them) the individual recovered files are encrypted but the re-created folder is not encrypted. Microsoft Windows documentation provides instructions on encrypting the re-created folder.
- Windows EFS encrypted data is backed up and recovered in its encrypted state.

## Event logs

Event logs can be used for troubleshooting hardware problems as well as monitoring security conditions, and system and application software problems.

If VSS is disabled, the NetWorker software backs up event logs for services that are running at the time of the backup. You can restore event logs to the same location or to a new location on the computer and then view them with the Microsoft Event Viewer.

The size of a restored event log might be smaller than the size of the corresponding backed-up log. This is characteristic of Windows event logs and does not cause any loss or modification of data. The recovered, smaller log can still be viewed in the Microsoft Event Viewer.

If more than one active event log is marked for backup (for example, SecEvent.Evt and SysEvent.Evt), all event logs are backed up.

Event logs can be recovered to a location different than the location from which they were backed up. However, event logs cannot be recovered to a FAT16 or FAT32 partition if they were backed up from an NTFS partition.

If VSS is enabled, event logs are backed as a component of the VSS SYSTEM SERVICES save set.

### **NOTICE**

---

Windows Server 2008 and Windows Vista do not have an event log writer. The event logs will not be backed up as part of the VSS system save sets. The event logs are backed up as part of the file system. To back up the event logs, perform a regular (non-VSS) backup of the system32\winevt\logs folder.

---

## Internet Information Server

Internet Information Server (IIS) is a web server that enables the publication of information on the Internet or a corporate intranet by using HTTP.

The NetWorker software uses the active metabase to back up IIS and can restore the backup versions to the metabase location. NetWorker supports the recover of the metabase to the default location %SystemRoot%\system32\inetsrv\MetaBase.bin or in a location that you specify in the registry. The Microsoft documentation provides information about how to creating a registry key that specifies an alternate metabase location.

### **NOTICE**

---

If you recover the VSS SYSTEM BOOT save set, and then reboot, the Network News Transfer Protocol (NNTP) virtual server may not start. To resolve this issue, rebuild the NNTP index and hash table files. The Microsoft NNTP documentation provides more information.

---

## Windows registry

The system state contains the Windows registry. The NetWorker software will automatically backup and restore the registry at a level full, as part of the VSS SYSTEM BOOT save set.

## Sparse files

The NTFS sparse files feature enables a program to create huge files without actually committing disk space for every byte. The NetWorker software provides complete backup and recovery support for sparse files.

## Advanced Configuration and Power Interface

NetWorker software uses the NetWorker Power Monitor service to provide Power Interface (ACPI), or OnNow support. The NetWorker software installation process configures the NetWorker Power Monitor service to start automatically when the other NetWorker services start. The binary for this service is located in *NetWorker\_install\_path \bin\nsrpm.exe*.

A scheduled backups requires that each client respond to a backup request by the NetWorker server. The NetWorker Power Monitor service prevents the NetWorker server or client host operating system and the network interface to enter the ACPI standby mode.

The NetWorker Power Monitor service does not prevent:

- A user from configuring a computer to power down to a standby state.
- Power-management policies from forcing the system to power down when line power is lost and the uninterrupted battery power reaches a critically low state.

The NetWorker software shuts down any storage management operation that is in progress when a user action forces a standby or when a critical power event occurs.

## Considerations for ACPI usage

Before you use ACPI, review the following conditions.

- Ensure that the NetWorker server host or client host is not in standby mode when either computer is to participate in a scheduled backup.
- Ensure that the NetWorker server and the target client are not in standby or hibernation mode during a backup or recovery operation. Doing so will yield unpredictable results.
- If you power down a NetWorker server while NetWorker operations are in progress, the peripheral devices may also powered down. If this occurs, when you power on the NetWorker server, the tape devices may rewind and NetWorker' server will have incorrect positioning information, which can result in data loss.

## Windows print queues

NetWorker will backup and recover print queues as a part of the file system and not as part of any VSS writer. During a recover operation, you may have to reboot the host depending on the status of the print queue at the time of the backup.

# Windows Optimized Deduplication

NetWorker supports backup of optimized data deduplication volumes and files and can restore optimized deduplication backups to a set of eligible restore targets.

NetWorker supports the data deduplication feature on Windows Server 2012, Windows Server 2012 R2, Windows Storage Server 2012 and Windows Storage Server 2012 R2. NetWorker does not support the feature on Windows 8 client computers or computers that run the older versions of the Windows operating system. On computers that run the Windows Server operating system, NetWorker supports the feature on volumes that use the NTFS file system, which can be part of a fail over cluster, including CSV volumes.

By default NetWorker performs an optimized deduplication backup on a optimized deduplication volume, unless the backup path is a subdirectory of the volume or when you specify the non-optimized deduplication save option in the Save operations field of the client resource. When you define the non-optimized deduplication save option, NetWorker will not deduplicate the backup. When the path is a subdirectory of a volume, NetWorker does not create an optimized backup.

To back up and restore Windows Server deduplication volumes or files, you must use a NetWorker 8.1 or later client. You can only restore deduplicated backups to computers that run on supported versions of Windows Server that have the data deduplication role enabled. The data deduplication role is a child role of File Services, which is a File and Storage Services role.

## Detecting Deduplication in a Backup

When a deduplication volume is backed up, you can verify the form of the data that was backed up. This information is identified in the mminfo extended save set attributes output. To show all extended save set attributes, use the mminfo output flag -r attrs. Deduplication backups are indicated with \*MSFT\_OPTIMIZEDDEDUP\_ENABLED:yes.

For more information on mminfo, refer to the *EMC NetWorker Command Reference Guide* or the mminfo man pages.

## Data Deduplication Backup and Restore

NetWorker supports two types of backup and four types of restores for data stored on a deduplication volume.

### Optimized full-volume backup

Optimized full-volume backups are the default backup type for Windows data deduplication volumes. The backup type occurs when the non-optimized data deduplication save option is not specified and the backup path is a mount point, drive letter or full volume backup. NetWorker full, incremental, and synthetic full backups are supported with Windows data deduplicated volumes.

The optimized data deduplication files that are part of the backup include:

- Windows data deduplication reparse points
- Chunk store containers and data deduplication meta data files

NetWorker backup does not differentiate whether a volume is configured for data deduplication, except to add the media database attribute if the volume is deduplicated. The media database attribute, \*MSFT\_OPTIMIZEDDEDUP\_ENABLED, is set to true and is saved as part of an optimized data deduplication volume save set.

For Windows BMR, the Windows Server 2012 and Windows Server 2012 R2 data deduplication writer is not part of the system state. Additionally, data deduplication volumes can be critical volumes and are supported with Windows BMR.

## Unoptimized full and incremental backup

NetWorker creates an unoptimized data deduplication backup under the following conditions:

- When you specify in the save set attribute of the client resource, a backup path that is a subdirectory of the volume, except in the case where the subdirectory is the root of a mount point.
- When you perform a manual backup of the client that does not make up the entire volume.
- When you specify the string VSS:NSRDEDUPNONOPTIMIZED=yes in the save operations settings of the client resource. If the save operation flag is set to yes the data deduplication backup is not optimized. If no string is present, or if the attribute is set to no, a normal volume level backup is performed.

To add this string:

From the NetWorker Administration console select Properties menu.

1. On the On the Client Properties text box, select the Apps & Modules tab.
2. In the Save operations field, enter the string and attribute setting and then click OK.  
In an unoptimized data deduplication backup, all files are rehydrated before the back up is performed. The deduplication chunk store directory is not backed up.  
Windows dedup backups, either optimized or unoptimized, will be corrupt if they are backed up with VSS off.

Reasons to create an unoptimized data deduplication volume backup include:

- Support restores of a Windows Server 2012 and Windows Server 2012 R2 backups to an earlier version of Windows Server.
- Support restores of a Windows Server 2012 Windows Server 2012 R2 backups to a non-Windows computer.

## Full volume restore to original path on the original computer

NetWorker supports a restore to the original volume mount path on the original server. All optimized files newer than the backup time of the restore save sets are rehydrated to prevent data loss.

When a deduplicated CSV volume is restored, CSV ownership is moved to the cluster node where the restore is being performed. This ensures that deduplication jobs and data access can be disabled during the restore process. The CSV is assigned back to original ownership when the restore is complete.

## Full volume restore to original path on a different computer

NetWorker supports a restore of a data deduplication backup from one computer to the same volume mount path on another compatible computer. Part of this type of restore includes validation checks to ensure that Windows Server 2012 or Windows Server 2012 R2 is installed on the target computer and that the deduplication role is enabled.

You can manually reformat the volume, but this is not a requirement for NetWorker. The restore can only take place if the volume does not have a pre-existing chunk store. Additionally, the volume will be enabled for data deduplication after the restore is complete.

## Support for save set restore of level FULL backups

A save set restore of a FULL backup is identical to a full volume restore with the following limitations:

- Limited to level Full backups in order to maintain chunk store integrity.
- Limited to volume level restores to the same path on the same computer where the backup was performed.
- No support for selective file restores due to insufficient information about the save set's restore context.

## File level restore

File level restore is performed if the volume to be restored is a subset of the original volume or if the restore is to a different volume. All files are restored in rehydrated form. The data deduplication meta data and chunk stores are not restored. For file level restores, the system account of the host where the restore is performed has to be a member of the NetWorker server's NetWorker Operators User Group. For example, if you are performing a dedup file level restore on host1, add system@host1 to the group.

**NOTICE**

If an optimized deduplication restore is aborted, it is likely to have mismatched reparse point and chunk store entries. This restored volume is not a valid restore. You must restore the backup again and allow the restore process to complete.

## Windows Data Deduplication Volume Best Practices

Review the following information, which describes the recommended best practices when you backup volumes that have Windows data deduplication enabled.

- A full backup should be performed immediately after deduplication has been enabled on a volume.
- Windows performs garbage collection on the chunk store of each deduplicated volume to remove no-longer-used chunks. By default, a garbage collection job is scheduled weekly for data deduplicated volumes. A full backup should be scheduled to run after garbage collection, because the garbage collection job may result in many changes in the chunk store, as a result of file deletions since the last garbage collection job.
- If there is significant chunk store container activity, control the size of incremental backups by limiting the frequency of Windows deduplication optimization jobs.
- Avoid performing extremely large file level restores. If a large percentage of a volume is restored, it is more time efficient to restore the entire volume. Because file level restores recover files in rehydrated form, a file level restore that includes many files might take up more space than is available on the volume.
- If a large file level restore is to be performed, first perform a full backup of the volume in its current state.
- When you choose to unoptimize many files at once from an optimized deduplication backup, the process can take a significant period of time. The selected files restore feature is best used to restore a moderate number of files. If most of a volume is to be restored, a full volume restore is a preferred solution. If a small amount of data needs to be skipped, that data can be moved to a temporary storage area, then back to its original location after the volume level restore is completed.

## Recommended Deduplication Workloads

Based on recommendations by Microsoft, the ideal workloads for data deduplication include:

- **General file shares:** Group content publication/sharing, user home folders and profile redirection (offline files)
- **Software deployment shares:** Software binaries, images, and updates
- **VHD libraries:** VHD file storage for provisioning to hypervisors

For NetWorker, AFTD device directories are good candidates for deduplication. AFTD directories contain a large number of redundant data blocks, which in general are infrequently accessed.

## APPENDIX C

# UNIX and Linux Platform-Specific Notes

This appendix contains the following topics:

• <a href="#">Solaris</a> .....	726
• <a href="#">Linux</a> .....	727
• <a href="#">HP-UX</a> .....	728
• <a href="#">AIX</a> .....	732

# Solaris

This section provides information specific to NetWorker software that runs on the Solaris platform.

## Solaris zone support

The NetWorker software provides support for local and global zones for a NetWorker client, server, and a dedicated storage node. You can install and back up a NetWorker client, server or storage node on a machine running in a local zone. [Dedicated storage nodes on page 130](#) provides more information about storage node support in a local zone.

**NOTICE**

---

The NetWorker Console (NMC) and the NetWorker License Manager can only be installed in a global zone.

## NetWorker executables not found for Solaris client

On Solaris, NetWorker executables are installed by default in `/usr/sbin`. If you start a group backup on a NetWorker server that does not have `/usr/sbin` in the search path for root, the backup fails on a client that has its NetWorker executables in `/usr/sbin`. This is because the `savefs` command is not in the search path.

To solve this issue, set the Executable Path attribute for the client or modify the search path for root on the NetWorker server to include `/usr/sbin`, even if the directory does not exist locally.

### Setting the Executable Path attribute

#### Procedure

1. From the **Administration** window, click **Configuration**.
2. In the expanded left pane, select **Clients**.
3. In the right pane, select the client name.
4. From the **File** menu, select **Properties**.
5. For the **Executable Path** attribute on the **Globals 2 of 2** tab, enter the path of the executables, `/usr/sbin`.
6. Click **OK**.

## Support for tape devices not supported by Solaris

For devices that are not directly supported by Sun Microsystems for use with your operating system, obtain a `st.conf` file from the device manufacturer.

## Extended file attribute data included in Save Set File Size attribute

The save set file size shown in NetWorker appears to be slightly larger than one might expect. This is because the extended file attribute data is included in the calculation of the save set file size.

## The inquire command and Solaris 10

On Solaris 10, the inquire command does not show library information after you configure the library for NetWorker.

## Improper font size for the Client Wizard with Netscape on Solaris

When you use the Netscape browser on Solaris, the font size may appear too small in the Client Wizard.

To change the font type and size, perform the following steps:

1. Open the `/usr/bin/nwwiz` script in a text editor.
2. Edit the following line to change the font size:

```
NSR_WIZARD_FONT_SIZE=size
```

3. Save and close the `nwwiz` file.

## Linux

This section provides information about NetWorker software that runs on the Linux platform.

### Backup considerations for Linux raw disk partitions

Review the following considerations before you attempt to back up a Linux raw disk partition.

- NetWorker can only save an unbound Linux raw device.
- In the Save set field for the Linux client, you must specify `/dev/sd` or `/dev/hd`.
- If you use the `/dev/raw` device, the backup fails.

### Configure Linux operating system to detect SCSI devices

Proper configuration of the SCSI subsystem is required to get full use of SCSI devices and allow the operating system to detect SCSI devices attached to the computer. If the device is configured with multiple LUNs, set the kernel parameter *Probe all LUNs of each SCSI Device* to **Yes**.

The *Linux Documentation Project* website provides more information on configuring the Linux SCSI subsystem. For information on the SCSI device, contact the manufacturer.

### The inquire command and the Scan for Devices operation do not detect more than 128 tape devices

By default, the Linux st kernel module will only configure up to 128 SCSI tape devices (`/dev/nst`).

When the number of SCSI tape devices exceeds the kernel value `ST_MAX_TAPES` the following error may be seen in the `/var/log/messages` operating system log file:

```
st:Too many tape devices (max. 128)
```

The `inquire` command or the **Scan for Devices** option in NMC will only display up to the number of st devices (`/dev/nst`) defined by the *ST\_MAX\_TAPES* value.

To resolve this issue, the st module of the Linux kernel must be modified and recompiled to increase the maximum number of allowable st devices created by the OS to exceed the default value. Refer to Linux documentation for details about how to reconfigure, rebuild, and install the kernel.

## Configuration requirements for the `inquire` command

Depending on the specific OS requirements, and the configuration of the NetWorker server or storage node, device files may need to be created so that the `inquire` command can detect all devices.

For example, on a NetWorker server that is running Red Hat Linux, if devices `sg0` through `sg15` already exist, create device file `sg16` by using the `mknod` program as follows:

```
mknod /dev/sg16 c 21 17
```

The operating system vendor documentation provides more information on creating devices.

## Linux Journaled file system support

Backup and recovery operations are supported on the following Linux journaled file systems:

- ext3
- reiserfs
- jfs
- xfs

**NOTICE**

For ext3 file systems with the journal set to visible, do not back up or recover the journal. Recovering the journal may cause the file system to become unstable. Use a directive to ensure that this file system is excluded from a backup. [Directives on page 269](#) provides information about directives.

## HP-UX

This section provides information specific to NetWorker storage nodesoftware that runs on the HP-UX platform.

### Autochanger installation on an HP-UX system

The following sections explain how to install and configure Hewlett-Packard drivers.

#### Selecting SCSI addresses for the autochanger

Determine which SCSI address is assigned to each SCSI bus and select the SCSI addresses to be allocated to the autochanger drives and controller.

To select unused SCSI addresses for an autochanger:

## Procedure

1. Log in as root on the NetWorker server or storage node and enter the **ioscan -f** command.
2. Use a SCSI address within the range of 0 to 6. The primary hard disk is usually on SCSI address 6.

**NOTICE**

For some devices, such as the HP Model 48AL autochanger, select one SCSI address for the entire autochanger. The 48AL uses a different SCSI logical unit number (LUN) for the device (LUN 0) and robotics (LUN 1). The SCSI LUN appears as the last digit of the H/W Path field in the ioscan output.

---

## Results

The following sections provide examples of the command and output to use with different combinations of hardware and operating systems.

## Installing the SCSI pass-through driver

The following procedure describes how to use SAM terminal mode to install a GSC, HSC, or PCI pass-through driver.

### Procedure

1. Select **Kernel Config** and press **Enter**.
2. Select **Drivers** and press **Enter**.
3. Select SCTL from the list. The SCSI\_ctl driver is represented by the name SCTL.
  - If the current state is in, proceed to step 9.
  - Select any unreserved name for the device. For example, do not select a name such as /dev/null.
4. From the **Actions** menu, select **Add Drivers to Kernel** and press **Enter**.
5. From the **Actions** menu, select **Create a New Kernel** and press **Enter**.
6. When prompted with “Are you sure?” indicate Yes, and press **Enter**.
7. The **Creating Kernel** message appears, followed by the Move Kernel Message. Select **OK** and press **Enter**. The system reboots.
8. Verify that the *spt* was successfully installed with the following command:

```
ioscan -kfn
```

9. Verify that the driver has claimed the autochanger. If the autochanger has been claimed, CLAIMED should appear under the S/W State header. If not, verify that the installation has been completed properly.
10. If the device entry was defined by the operating system, use the OS-defined entry and proceed to verify the installation.

## Determining the major number

To determine the value for *majornum*, type `lsdev -d sctl`

The output should resemble the following. The assigned number may differ from those displayed in this example:

Character HP-PB HSC or PCI	Block 75 203	spt -1	Driver sctl	spt	Class ctl
----------------------------------	--------------------	-----------	----------------	-----	--------------

The value for *majornum* is the number in the Character column.

## Determining the minor number

To determine the value for *minornum*, use the `ioscan` command. The relevant lines in the `ioscan` output are those:

- For the controller itself (which contains HP C6280-7000 in the Description column).
- For the adapter to which the controller is connected (which is the second line above the line for the controller and contains “ext\_bus” in the Class column).

If the `schgr` driver is configured on the system, it appears associated with the library. The `ioscan` output line resembles:

Class State spt CLAIMED	I H/W Type 0 DEVICE	H/W Path 10/4/4.6.0	Description schgr HP C6280-7000	Driver	S/W
----------------------------------	------------------------------	------------------------	---------------------------------------	--------	-----

If the `schgr` driver is not configured on the system, no driver appears to be associated with the library. The `ioscan` output line resembles:

Class S/W State unknown schgr C6280-7000	I H/W Type -1 UNCLAIMED	H/W Path 10/4/4.6.0	Description DEVICE	Driver Description	S/W
--	----------------------------------	------------------------	-----------------------	-----------------------	-----

## Testing the device driver and device file installation

After the device driver is installed and the device file is created, run the `inquire` command to list available SCSI devices.

### NOTICE

Use the `inquire` command with caution. Running `inquire` sends the SCSI inquiry command to all devices detected on the SCSI bus. Using `inquire` during normal operations may cause unforeseen errors and possible data loss may result.

An example of the output from this command (with the `-s` option) is as follows:

```
scsidev@0.1.0:HP          C1194F      0.14
Autochanger (Jukebox), /dev/rac/c0t1d0
scsidev@0.2.0:Quantum     DLT4000    CC37    Tape, /dev/rmt/
c0t2d0BESTnb
scsidev@0.3.0:Quantum     DLT4000    CC37    Tape, /dev/rmt/
c0t3d0BESTnb
scsidev@0.4.0:Quantum     DLT4000    CC37    Tape, /dev/rmt/
c0t4d0BESTnb
scsidev@0.5.0:Quantum     DLT4000    CC37    Tape, /dev/rmt/
c0t5d0BESTnb
```

As of HP-UX 11iv3, two different addressing modes are supported: LEGACY and AGILE. The inquire program lists devices using the B.T.L notation for the LEGACY addressing mode, for example:

```
scsidev@B.T.L.
```

For the AGILE addressing mode, it lists devices using the DSF notation, for example:

```
/dev/rtape/tape106_BESTnb
```

## Inquire command does not detect tape drive

When you attach a Tape drive to the HP-UX 11i V2 64-bit host and run the inquire command, the tape drive is not detected, even if the device is configured, labeled and mounted and a save was successful.

### Workaround

Identify the drive path in the /dev/rmt folder, and using this path configure the device, as usual.

Whenever a new device is attached to the system, ensure that the cached file /tmp/lgtoscsi\_devlist is updated. Remove this temp file and then run the inquire command, which will rebuild the file.

## Errors from unsupported media in HP tape drives

Certain HP tape drives can only read 4-mm tapes of a specific length. Some, for example, read only 60-meter tapes. To determine the type of tape that is supported, refer to the drive's hardware manual.

If unsupported media is used, the following types of error messages may appear in the specified situations:

- When the nsrmm or nsrjb command is used to label the tape:

```
nsrmm: error, label write, No more processes (5)
```

- When the scanner -i command is used:

```
scanner: error, tape label read, No more processes (11)
scanning for valid records ...
read: 0 bytes
read: 0 bytes
read: 0 bytes
```

## Unloading tape drives on an HP-UX server or storage node

When you use the nsrjb -u -S command to unload a tape drive in an autochanger that is attached to an HP-UX server or storage node, the unload operation ejects all of the tape volumes inside the autochanger devices and into their respective slots.

To unload a single drive to its corresponding slot, use the nsrjb -u -f devicename command instead.

## SCSI pass-through driver required for HP-UX autochangers

If an autochanger with a NetWorker HP-UX server is used, refer to the *EMC NetWorker Installation Guide*. Read the required procedures to follow before the jbconfig program is run. Even if the SCSI pass-through driver is installed, follow the procedures to rebuild the kernel. Then run the jbconfig program to configure the autochanger.

## Symbolic link entries in the fstab file

For HP-UX operating systems, do not use symbolic entries in the /etc/fstab file. If symbolic links are used in the fstab file, the NetWorker server will not back up the file system that the symbolic link points to.

## Customized backup scripts

On HP-UX, do not use the posix shell (/bin/sh) for customized backup scripts that are meant to be automatically started by the savegroup. Use the korn shell instead (/bin/ksh).

# AIX

This section provides information specific to NetWorker software that runs on the AIX platform.

## STK-9840 drives attached to AIX

If you attach an STK-9840 drive to an AIX server, use SMIT to modify the IBM tape drive definition field to set the value of Use Extended File Mark to Yes.

## LUS driver operation on AIX

The operation of the LUS driver on AIX has been changed with NetWorker release 7.6 SP2. When a library comes online, NetWorker now obtains an exclusive lock on the library. This lock is maintained as long as the library is enabled. As a result, diagnostic tools such as inquire and the sji utilities cannot be used to access the library during this time. To access the library using these tools, it will be necessary to take the library offline.

## Group ownership recovery

On AIX, non-root users who are performing a recovery, will not be able to restore group ownership (the set-group-id-on-execution or setuid permission bit) on binaries or files. This is expected behavior.

# APPENDIX D

## OS-X Support

This appendix contains the following topics:

- [Support for OS-X](#)..... 734
- [OS-X metadata support](#)..... 734
- [OS-X backup considerations](#)..... 734
- [Recovering files and directories from the command prompt](#)..... 736
- [Recovering files and directories by using the NetWorker Recover GUI](#)..... 737

## Support for OS-X

You can configure a OS-X host as a NetWorker client. You can use any supported NetWorker server on UNIX, Linux, or Windows to back up and restore an OS-X host. You cannot configure a OS-X host as a NetWorker server or an NMC server.

## OS-X metadata support

The NetWorker client for OS-X can backup and recover all file system metadata including:

- Finder information
- Resource forks
- Extended attributes
- Access Control Lists

## Supported file systems

The NetWorker client for OS-X software supports the following file systems:

- HFS+ (including journaled)
- HFS
- UFS

## OS-X backup considerations

Use this section to help plan successful backups for NetWorker clients on the OS-X platform.

## Scheduling a NetWorker client backup on OS-X

This section provides information on configuring backups for a NetWorker client on OS-X.

### Configuring an OS-X client with the required directive

To ensure a consistent state after a recovery operation, you must configure an OS-X to exclude certain files and directories from a backup.

#### Procedure

1. Create or edit the OS-X client resource. [Creating a backup Client resource on page 65](#) provides more information.
2. On the **General** tab, select one of the following directives from the **Directive** attribute list:
  - Mac OS Standard Directives
  - Mac OS with Compression Directives

[Preconfigured global directive resources on page 274](#) provides more information about the OS-X directives.
3. Click **OK**.

## Results

[Scheduled backups on page 60](#) provides more information about scheduling a backup.

## Performing a back up of the Open Directory for an OS-X server disaster recovery

Open Directory contains system configuration information that is essential for disaster recovery. The NetWorker Procedure Generator provides more information about disaster recovery.

The NetWorker Mac OS directives do not back up Open Directory database files. To ensure complete protection of a OS-X Server system in the event of a catastrophic failure, perform the following steps to back up the Open Directory database files.

### Procedure

1. Create or edit the OS-X client resource. [Creating a backup Client resource on page 65](#) provides information about creating a client resource.
2. On the **General** tab, make note of the name of the group selected in the **Group** attribute.
3. On the **Apps and modules** tab, in the **Backup Command** attribute, type **savepnpc**.

[Using the savepnpc command with a customized backup program on page 117](#) provides more information about enabling the Client resource to use the `savepnpc` command.

4. On the OS-X host, create a custom `savepnpc` script file in the `/nsr/res` directory with the name `group_name.res`.
- where `group_name` is the group that was selected for the client resource.

5. Edit the `savepnpc` script file and include the following entries:

- To back up LDAP directory domain for the Open Directory, type:

```
# slapcat -l /var/backups/networker.ldif
```

- To back up Password Server database for the Open Directory when the OS-X host uses LDAP over SSL, type:

```
# mkdir -p /var/backups/networker.odpdb
# mkpassdb -backupdb /var/backups/networker.odpdb
```

- To back up the local NetInfo directory domain, type:

```
# nidump -r / . > /var/backups/networker.nidump
```

---

### Note

Open Directory database files remain available during the backup.

## Example: Custom savepnpc script for OS-X

To back up the LDAP directory, Password Server, and NetInfo databases before each scheduled save on a OS-X client that is member of the Default group, perform the following steps:

1. In NMC, edit the properties of the client resource. On the **Apps and Modules** tab, in the **Backup command** field, type: **savepnpc**
2. Create the `/nsr/res/Default.res` script file with the following content:

```
type: savepnpc;
precmd: "/usr/sbin/slapcat -l /var/backups/networker.ldif;
```

```
/bin/mkdir -p /var/backups/networker.odpdb;
/usr/sbin/mkpassdb -backupdb /var/backups/networker.odpdb;
/usr/bin/nidump -r / . > /var/backups/networker.nidump"
```

## Performing a manual backup on OS-X

To perform a manual backup on a OS-X client, use the `save` command, in a Terminal session.

For example:

```
$ save "file_or_directory_to_back_up" -s NetWorker_server
```

---

### Note

If you do not specify the `-s NetWorker_server` option, the `save` command contacts the NetWorker server defined in the `/nsr/res/servers` file. The *NetWorker Command Reference Guide* provides more information about the `save` command.

## Recovering files and directories from the command prompt

Use the `recover` command to recover individual files and directories from the command prompt on a OS-X client.

The *EMC NetWorker Command Reference Guide* provides more information about the `recover` command.

### Procedure

- From the Mac OS-X Terminal application, type:

```
$ recover -s NetWorker_server
```

---

### Note

If you do not specify the `-s NetWorker_server` option, the `save` command contacts the NetWorker server defined in the `/nsr/res/servers` file.

- At the `recover` prompt:

- a. To browse the files and directories, use common UNIX shell commands such as `cd` and `ls`.
- b. To specify the files and directories that you want to recover, use the `add` command.

For example:

```
recover> add directory_name
```

- c. Optionally, to automatically overwrite existing files, use the `force` option at the `recover` prompt.
- d. To start the recovery operation, type `recover`:

```
recover> recover
```

**NOTICE**

Do not recover any OS-X operating system boot files. For example do not recover the OS-X operating system kernel, /mach\_kernel.

## Recovering files and directories by using the NetWorker Recover GUI

Use the NetWorker Recover application to recover data from a NetWorker server.

### Connecting to the NetWorker server

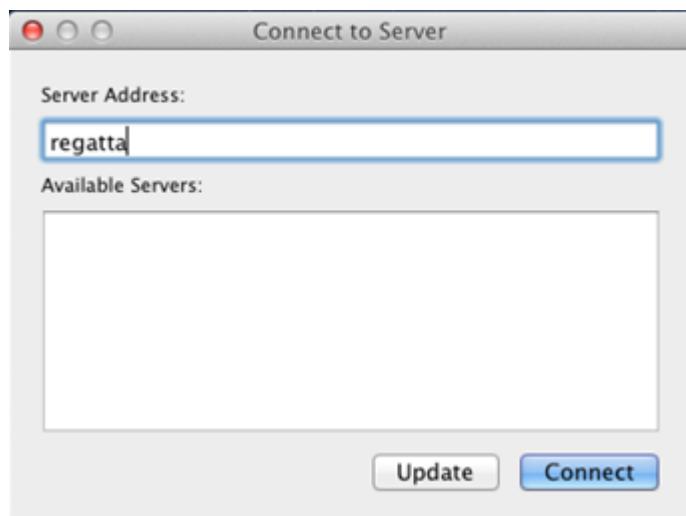
Perform the following steps on the OS-X client.

#### Procedure

1. Start the NetWorker Recover application.
  2. Use NMC to connect to the NetWorker server.
    - When you start the NetWorker Recover GUI for the first time, the **Connect to Server** dialog appears. Specify the NetWorker server that contains the backup data for the client:
      - In the **Available Servers** field, select the NetWorker server, and click **Connect**. The **Available Servers** field displays a list of host names that appear in the /nsr/res/servers file on the Mac client. To query the network for other NetWorker servers, click **Update**.
      - In the **Server Address** field, specify the hostname or IP address of the NetWorker server, and click **Connect**.
- The following figure shows the **Connect to Server** dialog.

#### Results

**Figure 47** Connect to Server

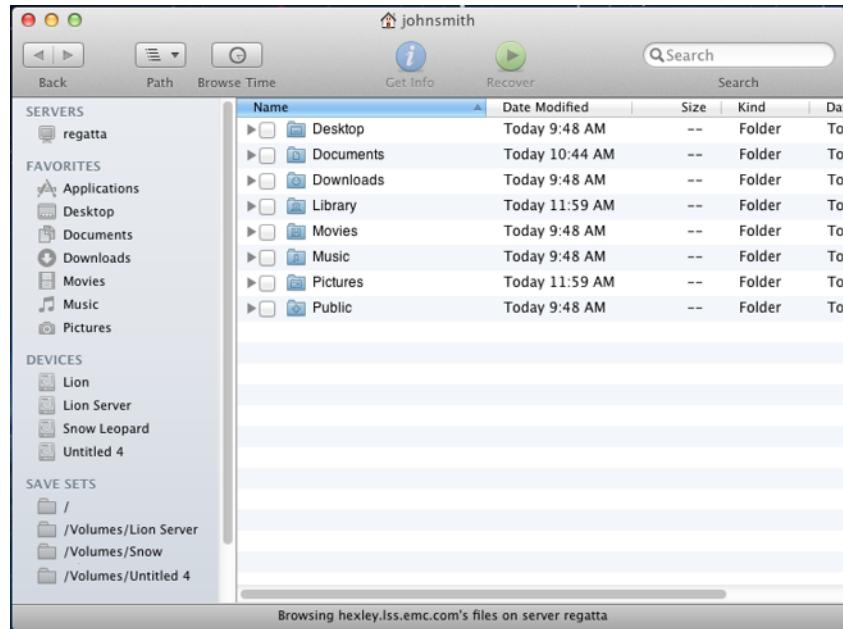


- When you close the NetWorker Recover GUI, subsequent recover operations will connect to the last NetWorker server selected, by default. To change the NetWorker server, perform one of the following steps:

**Figure 47** Connect to Server (continued)

- In the **SERVERS** section on the side bar, select the NetWorker server, then click **Connect**.
- On the **Go** menu, select **Connect to Server**. The **Connect to Server** dialog appears.

After you successfully connect to a NetWorker server, the **NetWorker Recover** window appears.

**Figure 48** NetWorker Recover window

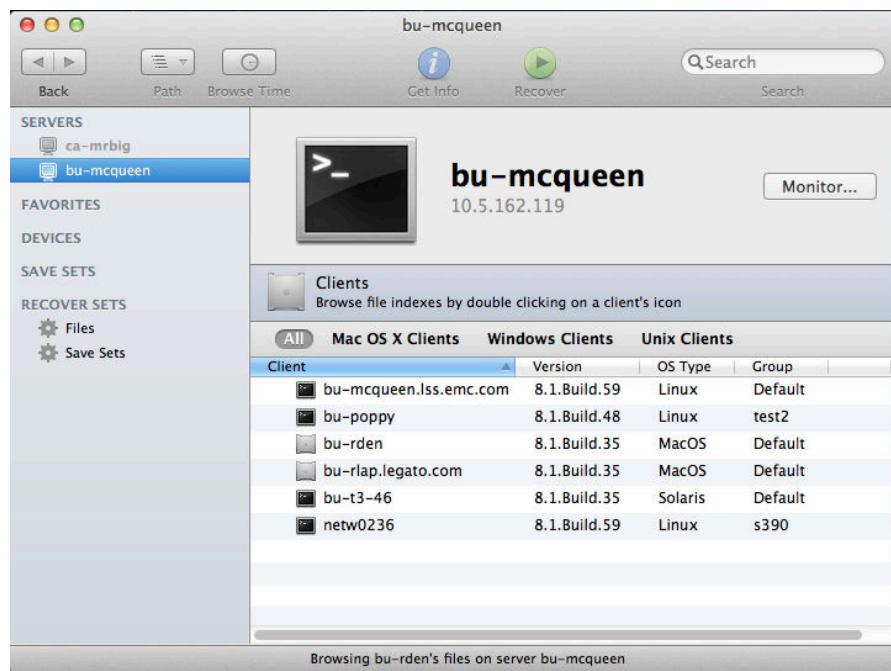
## Changing the source NetWorker Client

After you connect to the NetWorker server, the Browse view displays a list of files and folders that you can recover from the last local host backup.

NetWorker Recover provides you with the ability to recover of files from a host that is not the local host. [Directed recoveries on page 348](#) provides detailed information about directed recovery requirements.

To change the source host, perform one of the following actions:

- From the Go menu, select **Browse Client**. A list of clients for the current NetWorker server appear in a drop down. To establish a browse session with a new host, select the source host from the drop down.
- On the side bar, in the **SERVERS** section, select the NetWorker server. The browse view displays a list of clients. To establish a browse session with a new host, double-click the source host. The following figure provides an example of browse session window after you select a NetWorker server from the **SERVERS** section.

**Figure 49** List of clients available for a NetWorker server

#### Note

The Clients filter bar, located above the list of client names enables you to filter the client list by operating system. For example, select All to show all clients of the NetWorker server or select OS-X Clients to only display OS-X hosts.

## Changing the browse time

By default, the browser view displays files and directories from the last backup. To browse or recover files from an earlier backup, use one of the following methods to change the browse time:

- On the tool bar, select **Browse Time**. The **Browse Time** view appears, which displays the current browse time. Use the controls to specify a new date and time.
- From the **Go** menu, select **Browse Time**. Select one of the preconfigured options from the drop down. To use a calendar and clock to choose the date and time, select **Other**.

## Selecting objects to recover and recovering the data

NetWorker Recover supports the ability to perform a browsable recovery or a save set recovery.

#### Procedure

- Display a list of filesystem objects in the browser view.
- To perform a browsable recovery, on the side bar in the **Devices** section, select a filesystem. **NetWorker Recover** queries the client file index and displays the objects that you can recover.

**Note**

To show hidden files, from the **View** menu, select **Show Hidden Files**.

- To perform a save set recover, on the side bar in the **SAVE SETS** section, select a save set. NetWorker Recover queries the media database and displays each instance of the save set, including cloned save sets.

**Note**

The **Save Sets** filter bar, located above the list of save sets enables you to filter the save set list by save set type. For example, to show all of the original save set instances, select **Save Sets** or to only display cloned save set instances, select **Cloned Save Sets**.

2. To search browser view for the files you want to recover:
  - a. Type the text string in the **Search** field in the top right of the NetWorker Recover window.
  - b. Use the **Search Scope** bar to narrow the scope of your search result. The following figure displays some of the search criteria you can use.

**Figure 50** Search browse view

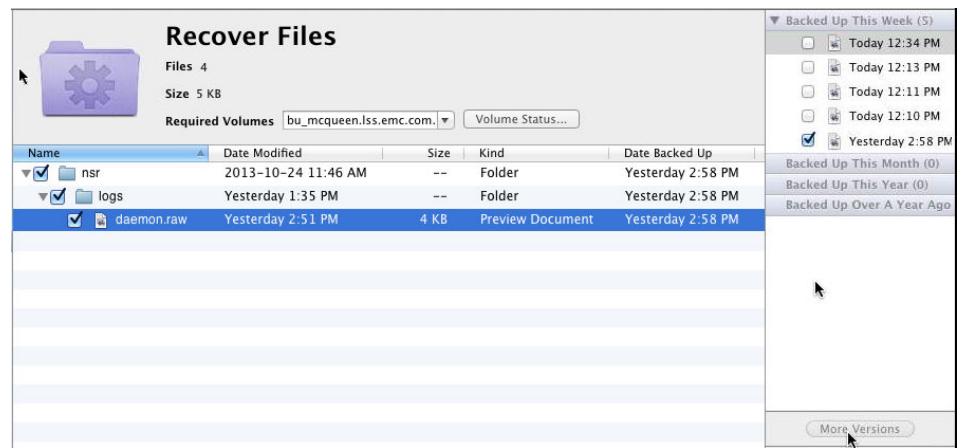


When you select an object in the **Search Result** view, NetWorker Recovery displays the path to the object in the Status bar at the bottom of the browser view.

3. To display information about an object, right-click the object and select **Get Info**.
4. To mark objects in the browser view for recovery, select the check box next to each object that you want to recover. You can only mark one save set or clone instance at a time.

NetWorker Recover adds each item that you mark to the **RECOVERY SETS** section on the side bar. A number appears next to each recovery set in the sidebar, which represents the total number of items selected for recovery.

5. To view or select different versions of a marked file, perform the following steps:
  - a. Right-click the file and select **File Versions**. The **Versions** side bar appears. The following figure provides an example of the **Versions** side bar.

**Figure 51** Versions side bar

- b. To recover a specific version of a file, perform one of the following actions:
  - Drag and drop the file from the **Versions** side bar to the browser view.
  - Drag the file to a folder for recovery.
  - Right-click the file to select **Mark for recovery**.
6. To review a summary list of the marked files, in the **RECOVERY SETS** section on the side bar, perform one of the following actions:
  - Select **Files** to display a list of objects that you marked for a browsable recovery.
  - Select **Save Sets** to display a list of objects that you marked for a save set recovery.

The **Recover Files** browse view displays a list of marked files and the list of volumes that the recovery operation requires.
7. To view the status of the required volumes, click **Volume Status**. Ensure that the status of the required volume(s) indicates on-line, then close the dialog.
8. To start the recover operation, the **Recover** button in the tool bar. The **Recover** window appears.
9. In the **Recover** window, select the recovery options.
  - To recover the objects to a directory that differs from the original location, perform one of the following actions:
    - In the **Relocate files to** field, type the path on the destination host to recover the data.
    - Click **Browse** and select the target directory.
  - Select a conflict resolution option:
    - Rename the recovered file. By default, the recover operation appends a tilde (~) to the beginning of the name of the recovered file ~file name. When a file named ~file name already exists, the recovered file is renamed ~00\_file name, and so forth to ~99\_file name. When this fails, the recover process does not automatically rename the file and prompts the user to specify a name for the file.
    - Discard recovered file: Discards the recovered file and keeps the existing file.
    - Replace local file: Replaces the file on the file system with the recovered version.

- Prompt me for an action: Each time the recovery operation encounters a file or folder with the same name in the destination location, the recovery operation prompts you to select a conflict resolution method.
- To recover the files to a different host, select the hostname from the **Direct recover to** drop down.
- Click **OK**. The recover status dialog appears. At any time during the recovery, you can click the **Stop** button to cancel the operation.

10.To monitor the recovery process, on the **Recover progress**, click the **Monitor Server**

The **NetWorker Monitor** dialog appears with the following tabs:

- Info—Displays general server information including name, IP, OS type, NetWorker version, Save totals and Recover totals.
- Messages—Displays server messages logged during the recovery, for example, errors and warnings.
- Devices—Displays the status for all connected devices.
- Sessions—Displays Save sessions, Recover sessions, and Browse sessions.
- Settings—Allows you to adjust the polling interval for server updates.

11.To review the recover log, after the recovery operation completes, select **Recover Log**.

The Console application appears and displays the contents of the `~/Library/Logs/recover.log` file.

## APPENDIX E

# Direct SCSI Backup and Recover

This appendix contains the following topics:

- [Introduction to direct SCSI backup and recover](#)..... 744
- [System requirements](#)..... 744
- [About direct SCSI backups](#)..... 745
- [About direct SCSI recovers](#)..... 747
- [Licensing Direct SCSI](#)..... 750

## Introduction to direct SCSI backup and recover

Direct SCSI backup and recover enables direct backup and recover of Small Computer System Interface (SCSI) devices without the requirement of mounting it on the backup host if an access path is available to these devices over a Storage Area Network (SAN). You can also use this feature to migrate EDM servers to the NetWorker software to perform backup and recover of Business continuance volume (BCV) devices on a Symmetrix server (as well as backup and recover of raw devices) over a SCSI bus.

Backup technologies often protect information as files and directories or as file systems. But backups also allow information contained on raw disks to be protected as raw devices. However, this type of backup (known as raw backup) usually does not provide granular recover capabilities.

The direct SCSI backup and recover feature enables raw backups for the NetWorker software directly by using a SCSI target, which is usually accessible from a SAN proxy host. Typically, in an EMC Symmetrix® storage environment, these devices can be viewed from a primary application host and from a proxy backup host. The direct SCSI backup and recover feature allows you to protect BCV devices from a proxy backup host as a raw backup.

Be aware that since backup and recover is performed on the proxy client (which is also a storage node), and a Symmetrix device is accessible, data is accessed from the proxy client, which may not be the client that originally created the data.

## System requirements

Before the configuration of Direct SCSI backup and restores, review the following list of requirements:

- The direct SCSI feature is only supported on Solaris SPARC storage nodes
- EMC Solution Enabler version 5.5 or later must be installed.
- The following hardware devices are supported:
  - Raw device path of a SCSI device
  - Sym

## Unsupported features

If performing backup and recover over a SCSI bus, the following features are not supported with NetWorker:

- Archiving
- Save set consolidation
- Index browsing
- Conventional recovery by using the command line recover utility
- File-by-file recovery
- Conventional save set recovery by using the command line recover utility

The EMC Symmetrix device is supported for use with SCSI backup and recover, but no other vendor device is supported with this feature as of NetWorker release 7.4.

## About direct SCSI backups

When performing Direct SCSI backup, you can perform either of the following:

- Single device backup
- Backup of a device set that consists of a list of devices specified in a resource file.

If the device is vendor-specific, the program loads the vendor-specific plug-in shared library.

The NetWorker software uses the nsrscsi\_save program to start the backup thread for each device to be backed up. Each backup thread performs the following operations:

- Finds the host accessible raw device path for the given vendor device.
- Starts a save session with the NetWorker server.
- Runs scsi asm on the raw device path to move data from the SCSI device to a storage node (nsrmmd) by using SCSI commands.

**NOTICE**

Before starting a backup, set the backup device to offline or read-only mode, and the file systems that reside on the device to read-only. If the device is a Symmetrix BCV, keep the BCV detached from the standard during the backup.

## Backing up data on a Symmetrix BCV device

To back up data on a Symmetrix BCV device:

### Procedure

1. Create the .res file (for example, /nsr/res/deviceset.res) if performing backup on a device set. Within the file, do the following:
  - a. Specify a list of devices to be backed up as part of a device set. Associate the device set with each entry in the file. You can identify the devices by their Symmetrix volume IDs (SYMMIDs) and category names, as in the following example:
 

```
000182504581/011 ## These two will be
000182504581/012 ## grouped as OracleDisks
# This is a comment line
000182504581/07D ## These two will be
000182504581/07E ## grouped as ExchDisks
```
  - b. Store this file in the *nsr/res* directory on the storage node.
2. For the AppHost or the host that controls the data, perform either of the following steps:
  - Create a new NetWorker Client resource. [Creating a backup Client resource on page 65](#) provides more information.
  - Edit an existing client by right-clicking the client in the Configuration screen of the Administration window and selecting Properties.

3. For the **Save Set** attribute, do one of the following:

- If performing multiple device backup, type the following:

`<>emc_symm>/<deviceset.res>`

where `<>emc_symm>` is the name of the device and `{deviceset.res}` is the name of the .res file.

- If performing single device backup without the .res file, type the following:  
`<<emc_symm>>`  
 where `<<emc_symm>>` is the name of the device.
4. On the **Apps and Modules** tab, select **SCSI** for the **Proxy backup type** attribute.
  5. In the **Proxy Backup host** attribute, enter the name of the storage node on which the `nsrscsi_save` command will be run.
  6. Click **OK**.

### Results

Once you create the Client resource, the `nsrscsi_save` program reads the .res file for all the device IDs listed or reads the ID for the single device, and starts the backup thread. The backup thread performs the following:

- validates the SYMMIDs
- finds the host-accessible raw device path for the SYMMIDs
- starts the save session with the NetWorker server.

The NetWorker software creates a save set for each category name, but does not create an index for the content within the BCV.

## Backing up data on a raw device

The process for backing up raw device data is similar to backing up data on a BCV device.

### Procedure

1. For the AppHost or the host that controls the data, perform either of the following steps:
  - Create a new NetWorker Client resource. [Creating a backup Client resource on page 65](#) provides more information.
  - Edit an existing client by right-clicking the client in the in the **Configuration** screen of the **Administration** window and selecting **Properties**.
2. For the **Save Set** attribute, type the path for the raw device with the device name. For example, if the device name is `c1t2d0s2` and the path is `/dev/rdsk`, type the following:

```
/dev/rdsk/c1t2d0s2
```

3. On the **Apps and Modules** tab, select **SCSI** for the **Proxy backup type** attribute.
4. In the **Proxy Backup host** attribute, enter the name of the storage node on which the `nsrscsi_save` command will be run.
5. Click **OK**.

### Results

Once you create the Client resource, associate it to scheduled group. At the scheduled time, the group starts the `nsrscsi_save` program on the storage node.

The `nsrscsi_save` program starts the backup thread. For a single device backup, a single backup thread is created by `nsrscsi_save`. The program starts the save session with the NetWorker server.

## Backing up data from the command line

To perform backup from the command line, run the following command:

```
nsrscsi_save [ -c clientname ] [ -g group ] [ -N save-set-name ] [ -I
input filename ] [ -s server ] [ -b pool ] [ -e expiration ] [ -y
retention time ] Path
```

where:

- **-c clientname** is the client name for starting the save session. The client name is the local host by default. If using the local host, you do not need to specify the client name.

### Note

The client-name is not necessarily the host accessible device. For example, a Symmetrix BCV device may be accessible on a different host for backup than the client where the standard device is attached (the client that you want to register the backup against).

- **-N save-set-name** is the name of the save set. The save set name is the pathname by default. If the pathname is the name of the device set, **-N** is ignored.
- **-I input-filename** is the filepathname for the file that contains the list of devices to be backed up (for example, /tmp/testdisks.res). If the input-filename is not specified, then the default input-filename is taken from device-set-name. For example, if the device-set-name is oracledisks, the input-filename would be /nsr/res/oracledisks.res. Also, if device-set-name is used in the path but **-I** is not specified, the default location is set to /nsr/res/device-set-name.res.
- The input file should contain only entries for the devices that need to be backed up. Multiple device entries should be separated by a new line. When **-I** is specified, device-set-name should also be specified.
- Path can be any of the following formats:
  - For a raw device path: /dev/rdsk/c1t2d0s2
  - For a device-set-name: {OracleDevices}
 Braces are required to distinguish device-set-name from a single device path.
- **-g group** is used by savegrp and savefs to specify the group of the save. It is also used by the NetWorker server to select the specific media pool.
- **-b pool** specifies a particular destination pool for the save. All the save sessions go to the same pool.

## About direct SCSI recoveries

Direct SCSI recover is performed by using the nsrscsi\_recover program. This program starts the recover thread for each save set to be recovered. From the command line, you can recover single save sets, or multiple save sets specified in a resource file, with a unique destination for each save set. If the device being recovered from is vendor-specific, the program loads the vendor-specific plug-in DLL.

Each recover thread performs the following operations:

- Finds the host accessible raw device path for the given target vendor device.
- Starts a recover session with the NetWorker server.

- Runs scsi asm on the raw device path to move data from the storage node (nsrmmmd) to a raw device via SCSI CDB commands.

**NOTICE**

Before starting the recovery, set the backup device to offline or read-only mode from the application host, and the file systems that reside on the device to read-only. If the device is a Symmetrix BCV, keep the BCV detached from the standard during the backup.

Also, note that the data on the target device being used for recovery will be rewritten and the original data will be lost when using the target device ID and raw device path for recovery.

## Recovering data to a Symmetrix BCV device

Recovering data on a Symmetrix BCV device must be performed from the command line. You cannot use NMC to perform this function.

### Procedure

- Perform an mminfo query on the device set name, for example:

```
mminfo -avVot -q "name=xxx"
```

The query returns a list of Save Set IDs (SSIDs) that are part of the device set.

- Find the SSID (for example, 3697521281), and then run the following command:

```
mminfo -aS -q "ssid=3697521281"
```

The list of connected save sets displays. The connected save sets are the save sets that are backed up as part of this device set.

- Select a save set from this list.
- If applicable, prepare the target device and retrieve the target vendor device ID. The target vendor device ID can be original.
- Run the following command:

- ```
1. nsrscsi_recover -S ssid -T target device
```

where ssid is the ID for the save set being recovered and target device is the SYMMID and the device ID (for example, 0034567/0366, where 0034567 is the SYMMID and 0366 is the device ID).

The NetWorker software recovers the contents of the save set to the destination location. The destination location is the original location by default.

To recover multiple save sets:

- Perform an mminfo query on the device set name. For example:

```
mminfo -avVot -q "name=xxx".
```

The query returns a list of Save Set IDs (SSIDs) that are part of the device set.

- Find the appropriate SSID (for example, 3697521281), and then run the following command:

```
mminfo -aS -q "ssid=3697521281",
```

The list of connected save sets displays. The connected save sets are the save sets that are backed up as part of this device set.

8. Choose the SSIDs from the list of connected save sets (in the following example, the SSIDs are 3697521281 and 3680744065):

```
mminfo -avVot -r "volume,name,savetime(25),ssid" | grep
oraclediskset
scip2b081.networker.com.001 oraclediskset:000187910217/0365
11/21/06 06:14:25 PM 3697521281
scip2b081.networker.com.001 oraclediskset:000187910217/0366
11/21/06 06:14:26 PM 3680744065
```

9. If applicable, prepare all target devices and retrieve the target vendor device IDs. The target vendor device ID can be the same as the original backup device ID.
10. Create a .res file under /nsr/res (for example, /nsr/res/restorelist.res), and specify an entry for each save set to be recovered.

Each entry in the .res file must have an SSID for every save set being recovered, mapped to a target device (SYMMID/Device ID), as in the following example:

```
3697521281=>000187910217/0366
3680744065=>000187910217/0365
```

11. Run the **recover** command:

```
nsrscsi_recover -I input filename
where input filename is the name and location of the .res file (for example, nsr/dev/restorelist.res).
```

Once you create the Client resource, the nsrscsi\_recover program reads the .res file for all the device IDs listed, and starts the recover thread. The recover thread validates the device IDs, finds the host-accessible raw device path for the IDs, and starts the recover session with the NetWorker server.

## Recovering data to a raw device

### Procedure

1. Perform an **mminfo** query and select an SSID (for example, 3697521281), as in the following example:

```
mminfo -aVvot
volume          client      size      level      name
ssid save       time        date      time       browse
clretent
first           last file   rec volid      total fl
scip2b081.networker.com.001 scip2b081.networker.com 8839 MB
full /dev/rdsk/c1t1d0s2
3697521281    1164161665    11/21/06 06:14:25 PM 12/21/06 11/21/07
0 9051405795    0 0 3731075692 9051405796 cr
```

2. If applicable, prepare the target device and retrieve the target raw device path. The target raw device path can be the same as the original raw device path.
3. Run the following command:

```
nsrscsi_recover -S ssid -T target device
where ssid is the ID for the save set being recovered and target device is the raw device path (for example, /dev/rdsk/c1t1d0s2).
```

The NetWorker software recovers the contents of the save set to the destination location. The destination location is the original location by default.

**NOTICE**

The destination path for recover must be specified and it must be a raw device or a vendor device.

---

## Licensing Direct SCSI

EMC Solution Enabler version 5.5 or later is required to use the Direct SCSI feature. There are no other licensing requirements for this feature.

# GLOSSARY

This glossary provides definitions for terms used in this guide.

## A

|                                          |                                                                                                                                                                                             |
|------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>access control list (ACL)</b>         | List that specifies the permissions assigned to a specific file or directory.<br><br><b>See</b> <a href="#">administrator</a>                                                               |
| <b>active group</b>                      | NetWorker backup group that has its Autostart attribute enabled.                                                                                                                            |
| <b>administrator</b>                     | Person who normally installs, configures, and maintains software on network computers, and who adds users and defines user privileges.                                                      |
| <b>Administrators group</b>              | Microsoft Windows user group whose members have the rights and privileges of users in other groups, plus the ability to create and manage the users and groups in the domain.               |
| <b>advanced file type device (AFTD)</b>  | Disk storage device that uses a volume manager to enable multiple concurrent backup and recovery operations and dynamically extend available disk space.                                    |
| <b>agent</b>                             | Term used by Sun Microsystems to denote a cluster server. Also known as a package (HP-UX), and a virtual server (Microsoft).                                                                |
| <b>annotation</b>                        | <ol style="list-style-type: none"><li>Comment associated with an archive save set.</li><li>Comment associated with an event.</li></ol>                                                      |
| <b>application specific module (ASM)</b> | Program that is used in a directive to specify how a set of files or directories is to be backed up or recovered. For example, compressasm is a NetWorker directive used to compress files. |
| <b>archive</b>                           | Process that backs up directories or files to an archive volume to free up disk space for regular backups. Archived data is not recyclable. <b>See</b> <a href="#">groom</a>                |
| <b>archive request</b>                   | NetWorker resource used to schedule and manage archiving.                                                                                                                                   |
| <b>archive volume</b>                    | Volume used to store archive data. Archive data cannot be stored on a backup volume or a clone volume.                                                                                      |
| <b>Atmos</b>                             | EMC cloud storage product.                                                                                                                                                                  |
| <b>attribute</b>                         | Name or value property of a resource.                                                                                                                                                       |
| <b>authentication</b>                    | Process by which a user or software process is determined to be trusted or not trusted.                                                                                                     |
| <b>authorization</b>                     | Privileges assigned to users.                                                                                                                                                               |
| <b>authorization code</b>                | Unique code that in combination with an associated enabler code unlocks the software for permanent use on a specific host computer. <b>See</b> <a href="#">license key</a>                  |

**autochanger** See [library](#)

**auto media management** Feature that enables the storage device controlled by the NetWorker server to automatically label, mount, and overwrite a volume it considers unlabeled.

## 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 cycle** Full or level 0 backup and all the subsequent incremental backups that are dependent on that backup.

**Backup Operators group** Microsoft Windows user group whose members have the capability to log in to a domain from a workstation or a server, whose data they may back up and restore. Backup Operators can also shut down servers or workstations.

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

**bootstrap** Save set that is essential for disaster recovery procedures. The bootstrap consists of three components that reside on the NetWorker server: the media database, the resource database, and a server index.

**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. See [retention policy](#)

## C

**canned report** Preconfigured report that can be tailored by the user.

**carousel** See [library](#)

**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.

**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 that is indexed and tracked by the backup server. Single save sets or entire volumes can be cloned.  
2. Type of mirror that is specific to a storage array.

|                                           |                                                                                                                                                                                                                                                                                                                                     |
|-------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>clone volume</b>                       | Exact duplicate of a backup or archive volume. NetWorker software can index and track four types of volumes (backup, archive, backup clone, and archive clone). Save sets of these different types may not be intermixed on one volume. Clone volumes may be used in exactly the same way as the original backup or archive volume. |
| <b>cloud</b>                              | Configuration of backup disks that uses EMC Atmos.                                                                                                                                                                                                                                                                                  |
| <b>cluster</b>                            | 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.                                                                                                                                                                 |
| <b>common internet file system (CIFS)</b> | Formerly known as Server Message Block (SMB). Message format used by Microsoft DOS and Windows to share files, directories, and devices.                                                                                                                                                                                            |
| <b>connection port</b>                    | Port used to perform functions through a firewall.                                                                                                                                                                                                                                                                                  |
| <b>Console application administrator</b>  | Console server user role whose members can configure features, except security features, in the Console sever application.                                                                                                                                                                                                          |
| <b>Console security administrator</b>     | Console server user role whose members can add Console users and assign them to Console roles.                                                                                                                                                                                                                                      |
| <b>Console server</b>                     | See <a href="#">NetWorker Management Console (NMC)</a>                                                                                                                                                                                                                                                                              |
| <b>consolidate</b>                        | To create a full backup by merging a new level 1 backup with the last full level backup.                                                                                                                                                                                                                                            |
| <b>continued save set</b>                 | Save set data that is continued from a previous volume.                                                                                                                                                                                                                                                                             |
| <b>control zone</b>                       | Group of datazones managed by the NetWorker software.                                                                                                                                                                                                                                                                               |
| <b>conventional storage</b>               | Storage library attached to the NetWorker server or storage node, used to store backups or snapshot backups. Also known as secondary storage. See <a href="#">primary storage</a>                                                                                                                                                   |

## D

|                                          |                                                                                                                                                                                                                                                                                                                                               |
|------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>daemon</b>                            | Process on UNIX systems that runs in the background and performs a specified operation at predefined times or in response to certain events.                                                                                                                                                                                                  |
| <b>database</b>                          | <ol style="list-style-type: none"> <li>1. Collection of data arranged for ease and speed of update, search, and retrieval by computer software.</li> <li>2. Instance of a database management system (DBMS), which in a simple case might be a single file containing many records, each of which contains the same set of fields.</li> </ol> |
| <b>data management application (DMA)</b> | Application that manages a backup or recovery session through an NDMP connection.                                                                                                                                                                                                                                                             |
| <b>data mover (DM)</b>                   | Client system or application, such as NetWorker software, that moves data during a backup, recovery, snapshot, or migration operation. <i>See also</i> <a href="#">proxy host</a> .                                                                                                                                                           |
| <b>data server agent (DSA)</b>           | Functionality that enables the NetWorker server to communicate with a non-NetWorker NDMP host and package images of save streams. For example, an NDMP host that generates proprietary save data may send that data to a NetWorker storage device to have a save set associated with it.                                                      |

|                                      |                                                                                                                                                                                                                                                                                                                                                                          |
|--------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>data service provider (DSP)</b>   | Feature that controls access to disk storage during an NDMP back up.                                                                                                                                                                                                                                                                                                     |
| <b>datazone</b>                      | Group of clients, storage devices, and storage nodes that are administered by a NetWorker server.                                                                                                                                                                                                                                                                        |
| <b>deduplication backup</b>          | Type of backup that removes redundant blocks of data to decrease storage space usage. When the deduplication data is restored, the data is returned to its original native format.                                                                                                                                                                                       |
| <b>destination client</b>            | Computer to which database files are restored in a directed recovery.                                                                                                                                                                                                                                                                                                    |
| <b>device</b>                        | <ol style="list-style-type: none"> <li>1. Storage unit or folder that can contain a backup volume. A device can be a tape, optical drive, autochanger, or disk connected to the server or storage node.</li> <li>2. General term that refers to storage hardware.</li> <li>3. Access path to the physical drive, when dynamic drive sharing (DDS) is enabled.</li> </ol> |
| <b>Device Central</b>                | Interface from which one can manage all NetWorker libraries.                                                                                                                                                                                                                                                                                                             |
| <b>DFS component</b>                 | <ol style="list-style-type: none"> <li>1. A namespace for files and DFS links, called a DFS root.</li> <li>2. A connection to a shared file or folder, called a DFS child node.</li> </ol> <p><b>See</b> <a href="#">distributed File System (DFS)</a></p>                                                                                                               |
| <b>direct access restore (DAR)</b>   | NDMP operation that can recover data in the middle of a tape set without having to parse the tape set sequentially, thereby reducing the recovery time of large backups.                                                                                                                                                                                                 |
| <b>directed recovery</b>             | Method that recovers data that originated on one client host and re-creates it on a different client host, known as the destination client.                                                                                                                                                                                                                              |
| <b>directive</b>                     | Instructions to take special actions on a given set of files for a specified client during a backup.                                                                                                                                                                                                                                                                     |
| <b>disaster recovery</b>             | Restore and recovery of data and business operations in the event of hardware failure or software corruption.                                                                                                                                                                                                                                                            |
| <b>distributed File System (DFS)</b> | Microsoft Windows add-on that creates a logical directory of shared directories that span multiple hosts across a network.                                                                                                                                                                                                                                               |
| <b>document mode</b>                 | Display mode that presents static reports such as charts or tables in a format that resembles the Print Preview mode in a PDF viewer.                                                                                                                                                                                                                                    |
| <b>domain controller</b>             | Server that stores directory data and manages user access to a network.                                                                                                                                                                                                                                                                                                  |
| <b>drill-down</b>                    | Organization of report information by granularity. For example, within a group summary report, a client report may be viewed, and then a report for a selected save set for that client.                                                                                                                                                                                 |
| <b>drive</b>                         | Hardware device through which media can be read or written to. <b>See</b> <a href="#">device</a>                                                                                                                                                                                                                                                                         |
| <b>DSA save set</b>                  | Save sets of an NDMP client that are backed up to non-NDMP tape device. <b>See</b> <a href="#">data server agent (DSA)</a>                                                                                                                                                                                                                                               |
| <b>dynamic drive sharing (DDS)</b>   | Feature that allows NetWorker software to recognize and use shared drives and when they are available.                                                                                                                                                                                                                                                                   |

## E

|                           |                                                                                                                                                                                                                                                                                                      |
|---------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>enabler code</b>       | Unique code that activates the software:                                                                                                                                                                                                                                                             |
|                           | <ul style="list-style-type: none"> <li>• Evaluation enablers or temporary enablers expire after a fixed period of time.</li> <li>• Base enablers unlock the basic features for software.</li> <li>• Add-on enablers unlock additional features or products, for example, library support.</li> </ul> |
|                           | <b>See</b> <a href="#">license key</a>                                                                                                                                                                                                                                                               |
| <b>enterprise</b>         | Computers and folders organized into a tree-based visual representation.                                                                                                                                                                                                                             |
| <b>event</b>              | Notification generated by an application that could require user action, such as the impending expiration of a software enabler key that appears in the daemon log of the Console server.                                                                                                            |
| <b>event-based backup</b> | <b>See</b> <a href="#">probe-based backup</a>                                                                                                                                                                                                                                                        |
| <b>exit code</b>          | Indicator that specifies whether a backup or recovery session succeeded. An exit code of zero (0) indicates the session completed successfully. A nonzero exit code indicates that the session did not complete successfully.                                                                        |
| <b>expiration date</b>    | Date when a volume changes from read/write to read-only.                                                                                                                                                                                                                                             |
| <b>expired save set</b>   | Save set that has exceeded its browse time and has been removed from the NetWorker client file index. Expired save sets can no longer be browsed.                                                                                                                                                    |

## F

|                    |                                                                                                                                                                                                                                                                                             |
|--------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>file index</b>  | <b>See</b> <a href="#">client file index</a>                                                                                                                                                                                                                                                |
| <b>file system</b> | <ol style="list-style-type: none"> <li>1. Software interface used to save, retrieve, and manage files on storage media by providing directory structures, data transfer methods, and file association.</li> <li>2. Entire set of all files.</li> <li>3. Method of storing files.</li> </ol> |
| <b>firewall</b>    | Security software designed to prevent unauthorized access to or from a private network.                                                                                                                                                                                                     |
| <b>folder</b>      | An icon on a computer screen that can be used to access a directory.                                                                                                                                                                                                                        |
| <b>full backup</b> | Type of backup that backs up all data objects or files, including the transaction logs contained in databases, regardless of when they last changed. <b>See</b> <a href="#">level</a>                                                                                                       |

## G

|                                       |                                                                                                 |
|---------------------------------------|-------------------------------------------------------------------------------------------------|
| <b>generic services toolkit (GST)</b> | Software framework that underlies the Console server.                                           |
| <b>groom</b>                          | Process that removes the original files from a local disk after a successful archive operation. |

**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

**hash** Number generated from a string of text that is used to encrypt a user password. [See salted hash](#)

**heterogeneous network** Network with systems of different platforms and operating systems that interact across the network.

**high-availability system** System of multiple computers configured as cluster nodes on a network that ensures the application services continue despite a hardware or software failure.

**high-water mark** Percentage of disk space that, when filled, automatically starts the staging process.

**host** Computer on a network.

**host authentication** Encryption and verification services between NetWorker hosts. [See user authentication](#)

**host ID** Eight-character alphanumeric number that uniquely identifies a computer.

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

## I

**inactivity timeout** Time in minutes to wait before a client is considered to be unavailable for backup.

**incremental backup** [See level](#)

**individual user authentication** Process by which Console administrators restrict or grant user access to NetWorker servers, based on Console usernames.

**insertion time** Time that the save set record was most recently introduced into the save set database.

**Interactive mode** Console mode that displays reports (as charts or tables) that users can interact with. For example, one can sort, rearrange, and resize columns in a table-format report that was run in this mode.

**internationalization (I18N)** Capability of the software to display and output data in the same language fonts and numeric formats that are passed to it by localized operating systems or applications.

## J

**Java** Type of high-level programming language that enables the same, unmodified Java program to run on most computer operating systems. [See Java Virtual Machine \(JVM\)](#)

**Java archive (JAR)** File that contains compressed components needed for a Java applet or application.

**Java plug-in** JVM that can be used by a web browser to run Java applets.

|                                                     |                                                                                                                                                                                                                                                                                                                                                                      |
|-----------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Java Virtual Machine (JVM)</b>                   | Execution environment for interpreting the Java programming language. Each operating system runs a unique JVM to interpret Java code.                                                                                                                                                                                                                                |
| <b>jukebox</b>                                      | <a href="#">See library</a>                                                                                                                                                                                                                                                                                                                                          |
| <b>L</b>                                            |                                                                                                                                                                                                                                                                                                                                                                      |
| <b>label</b>                                        | Electronic header on a volume used for identification by a backup application.                                                                                                                                                                                                                                                                                       |
| <b>legacy method</b>                                | Use of special-case Microsoft APIs to back up and recover operating system components, services, and applications.                                                                                                                                                                                                                                                   |
| <b>level</b>                                        | Backup configuration option that specifies how much data is saved during a scheduled or manual backup: <ul style="list-style-type: none"> <li>• A full backup backs up all data objects or files, regardless of when they last changed.</li> <li>• An incremental backup backs up only data objects or files that have changed since the previous backup.</li> </ul> |
| <b>library</b>                                      | Hardware device that automates the loading and mounting of movable storage media during backup and recovery processes. The term library is synonymous with autochanger, autoloader, carousel, datawheel, jukebox, and near-line storage.                                                                                                                             |
| <b>library sharing</b>                              | Shared access of servers and storage nodes to the individual tape drives within a library. The drives are statically assigned to hosts.                                                                                                                                                                                                                              |
| <b>license key</b>                                  | Combined enabler code and authorization code for a specific product release to permanently enable its use. Also called an activation key or license enabler.                                                                                                                                                                                                         |
| <b>License Manager (LLM)</b>                        | Application that provides centralized management of product licenses.                                                                                                                                                                                                                                                                                                |
| <b>Lightweight Directory Access Protocol (LDAP)</b> | Set of protocols for accessing information directories.                                                                                                                                                                                                                                                                                                              |
| <b>live backup</b>                                  | <a href="#">See rollover-only backup</a>                                                                                                                                                                                                                                                                                                                             |
| <b>local cluster client</b>                         | NetWorker client that is not bound to a physical machine, but is instead managed by a cluster manager. It is also referred to as a logical or virtual client.                                                                                                                                                                                                        |
| <b>localization (L10N)</b>                          | Translation and adaptation of software for the user language, time formats, and other conventions of a specific locale.                                                                                                                                                                                                                                              |
| <b>logical cluster client</b>                       | <a href="#">See virtual cluster client</a>                                                                                                                                                                                                                                                                                                                           |
| <b>logical device</b>                               | Virtual device used in the integration of NetWorker software with SmartMedia or AlphaStor. Many logical devices can be assigned to a single physical device.                                                                                                                                                                                                         |
| <b>low-water mark</b>                               | Percentage of disk space filled that, when reached, automatically stops the migration process.                                                                                                                                                                                                                                                                       |
| <b>LUS</b>                                          | Driver used by EMC software products as a proprietary device driver that sends arbitrary SCSI commands to an autochanger. Also known as the EMC User SCSI.                                                                                                                                                                                                           |

**M**

|                            |                                                                                                                                                                                    |
|----------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>managed application</b> | Program that can be monitored or administered, or both from the Console server.                                                                                                    |
| <b>managed node</b>        | Storage management application under the control of Console. For example, a system running NetWorker on a backup server or storage node is considered to be a managed node.        |
| <b>man pages</b>           | Online technical reference manual, normally provided on UNIX servers, for the syntax and function of program commands that may be issued from the command line.                    |
| <b>manual backup</b>       | Backup that a user performs from the client, also known as an unscheduled, on-demand, or ad hoc backup.                                                                            |
| <b>media</b>               | Physical storage, such as a disk file system or magnetic tape, to which backup data is written. See <a href="#">volume</a>                                                         |
| <b>media index</b>         | Database that contains indexed entries of storage volume location and the life cycle status of all data and volumes managed by the NetWorker server. Also known as media database. |
| <b>member</b>              | Physical host that occupies a node in a cluster environment. Each member has its own IP address.                                                                                   |
| <b>mount</b>               | To make a volume physically available for use such as the placement of a removable tape or disk volume into a drive for reading or writing.                                        |
| <b>mount host</b>          | Host in a network that is used to mount storage array snapshot volumes to perform snapshot restore and rollover operations.                                                        |
| <b>mount point</b>         | See <a href="#">volume mount point</a>                                                                                                                                             |
| <b>multiple session</b>    | Method of backing up or restoring multiple parallel streams of data simultaneously between a database and multiple storage devices. Also known as multistripe.                     |
| <b>multiplex</b>           | To simultaneously write data from more than one save set to the same storage device.                                                                                               |

**N**

|                          |                                                                                                                                                                                                                                                                                                                                                                                                 |
|--------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>NDMP server</b>       | Instance of one or more NDMP services, such as a data, tape, or SCSI server, that is managed by a single control connection.                                                                                                                                                                                                                                                                    |
| <b>NDMP service</b>      | Virtual machine that is controlled by a data management application (DMA) such as NetWorker software. Example services include: <ul style="list-style-type: none"> <li>• Server with a directly attached storage appliance</li> <li>• Storage device system with one or more tape drives</li> <li>• Software process that reads two datastreams and multiplexes them into one stream</li> </ul> |
| <b>NDMP storage node</b> | Host or open system with NDMP services. For example, Netapp Filer and EMC Filer.                                                                                                                                                                                                                                                                                                                |
| <b>near-line storage</b> | See <a href="#">library</a>                                                                                                                                                                                                                                                                                                                                                                     |

|                                                |                                                                                                                                                                                                                                                      |
|------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>network attached storage (NAS)</b>          | Disk array or storage device (NAS filer) that connects directly to the messaging network or LAN interfaces and uses the common communication protocols of either TCP/IP or NDMP.                                                                     |
| <b>network data management protocol (NDMP)</b> | 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.                                                        |
| <b>NetWorker administrator</b>                 | NetWorker server user who may add, change, or delete NetWorker server users.                                                                                                                                                                         |
| <b>NetWorker application administrator</b>     | NetWorker server user who may operate NetWorker software, configure the NetWorker server, and create and modify NetWorker resources.                                                                                                                 |
| <b>NetWorker Management Console (NMC)</b>      | Software program that is used to manage NetWorker servers and clients. The NMC server also provides reporting and monitoring capabilities for all NetWorker processes.                                                                               |
| <b>NetWorker security administrator</b>        | NetWorker server user who may add, change, or delete NetWorker server user groups.                                                                                                                                                                   |
| <b>NetWorker server</b>                        | 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.                                                           |
| <b>NetWorker Snapshot Management</b>           | 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. |
| <b>network file system (NFS)</b>               | Communications protocol that enables users to access shared files on different types of computers over a network.                                                                                                                                    |
| <b>NFS server</b>                              | Host that contains exported file systems that NFS clients can access. See <a href="#">network file system (NFS)</a>                                                                                                                                  |
| <b>node</b>                                    | See <a href="#">cluster</a>                                                                                                                                                                                                                          |
| <b>noncritical volume</b>                      | Volume that contains files that are not part of the system state or an installed service.                                                                                                                                                            |
| <b>notification</b>                            | Message sent to the NetWorker administrator about important NetWorker events.                                                                                                                                                                        |
| <b>nsrd</b>                                    | Master NetWorker server process.                                                                                                                                                                                                                     |
| <b>nsrhost</b>                                 | Logical hostname of the NetWorker server.                                                                                                                                                                                                            |

## O

|                        |                                                                                                                                                       |
|------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>offline backup</b>  | Backup of database objects performed while the corresponding database or instance is shut down and unavailable to users. Also known as a cold backup. |
| <b>offline restore</b> | Automated restore that does not require the manual installation of an operating system. A bare metal recovery (BMR) is an offline restore.            |
| <b>online backup</b>   | Backup of database objects performed while the corresponding database or instance is running and available to users. Also known as a hot backup.      |

|                       |                                                                                                                                                                                                  |
|-----------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>online indexes</b> | Databases located on the NetWorker server that contain all the information pertaining to the client backups (client file index) and backup volumes (media index).                                |
| <b>online restore</b> | Restore operation that is performed from a NetWorker recover program. An online restore requires that the computer has been booted from an installed operating system. See also offline restore. |
| <b>operator</b>       | Person who performs day-to-day data storage tasks such as loading backup volumes into storage devices, monitoring volume locations and server status, verifying backups, and labeling volumes.   |
| <b>override</b>       | Different backup level that is used in place of the regularly scheduled backup.                                                                                                                  |

## P

|                                      |                                                                                                                                                                                                                                                                                                                                                 |
|--------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>package</b>                       | A term used by HP-UX to denote a cluster server. Also known as an agent (Sun) or virtual server (Microsoft).                                                                                                                                                                                                                                    |
| <b>parallelism</b>                   | Method that backs up or recovers data for multiple clients, or multiple save sets for one client, at the same time.                                                                                                                                                                                                                             |
| <b>pathname</b>                      | Set of instructions to the operating system for accessing a file: <ul style="list-style-type: none"> <li>An absolute pathname indicates how to find a file by starting from the root directory and working down the directory tree.</li> <li>A relative pathname indicates how to find a file by starting from the current location.</li> </ul> |
| <b>peer</b>                          | NetWorker host that is involved in an authentication process with another NetWorker host.                                                                                                                                                                                                                                                       |
| <b>permanent enabler</b>             | Enabler code that has been made permanent by the application of an authorization code. <b>See</b> <a href="#">enabler code</a>                                                                                                                                                                                                                  |
| <b>physical cluster client</b>       | Backup client that is bound to a physical host in the cluster and can have its own resources (private or local).                                                                                                                                                                                                                                |
| <b>physical host</b>                 | Node or host that forms part of a cluster.                                                                                                                                                                                                                                                                                                      |
| <b>point-in-time copy (PIT copy)</b> | 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.                                                                                                    |
| <b>policy</b>                        | Set of defined rules for client backups that can be applied to multiple groups. Groups have dataset, schedule, browse, and retention policies.                                                                                                                                                                                                  |
| <b>pool</b>                          | <ol style="list-style-type: none"> <li>NetWorker sorting feature that assigns specific backup data to be stored on specified media volumes.</li> <li>Collection of NetWorker backup volumes to which specific data has been backed up.</li> </ol>                                                                                               |
| <b>primary storage</b>               | Server storage subsystem, such as a disk array, that contains application data and any persistent snapshots of data. <b>See</b> <a href="#">conventional storage</a>                                                                                                                                                                            |

|                           |                                                                                                                                                                                                     |
|---------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>probe-based backup</b> | Type of scheduled backup, also known as an event-based backup, where the NetWorker server initiates the backup only when specified conditions are met, as determined by one or more probe settings. |
| <b>proxy host</b>         | Surrogate host computer that performs backup or clone operations in place the production host by using a snapshot copy of the production data. <a href="#">See mount host</a>                       |
| <b>purge</b>              | Operation that deletes file entries from the client file index.                                                                                                                                     |

**Q**

|                |                                                                                                                                                                                                               |
|----------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>quiesce</b> | State in which all writes to a disk are stopped and the filesystem cache is flushed. Quiescing the database prior to creating the snapshot provides a transactionally consistent image that can be remounted. |
|----------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|

**R**

|                                    |                                                                                                                                                                                                                                                                                      |
|------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>recover</b>                     | 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.                                                                                                                                |
| <b>recyclable save set</b>         | Save set whose browse and retention policies have expired. Recyclable save sets are removed from the media database.                                                                                                                                                                 |
| <b>recyclable volume</b>           | Storage volume whose data has exceeded both its browse and retention policies and is now available to be relabeled and reused.                                                                                                                                                       |
| <b>Registry</b>                    | Microsoft Windows database that centralizes all Windows settings and provides security and control of system, security, and user account settings.                                                                                                                                   |
| <b>remote device</b>               | <ol style="list-style-type: none"> <li>1. Storage device that is attached to a storage node that is separate from the NetWorker server.</li> <li>2. Storage device at an offsite location that stores a copy of data from a primary storage device for disaster recovery.</li> </ol> |
| <b>remote procedure call (RPC)</b> | Protocol used by the backup server to perform client requests over a network.                                                                                                                                                                                                        |
| <b>repository</b>                  | Console database that contains configuration and reporting information.                                                                                                                                                                                                              |
| <b>requestor</b>                   | A VSS-aware application that creates and destroys a shadow copy. NetWorker software is a requestor. <a href="#">See shadow copy</a>                                                                                                                                                  |
| <b>resource</b>                    | 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.                                                                            |
| <b>resource database</b>           | NetWorker database of information about each configured resource.                                                                                                                                                                                                                    |
| <b>resource owner</b>              | Logical cluster host that owns the resource. If a Cluster resource, such as a shared disk, is not owned by a virtual host, it is assumed to be owned by the physical node that hosts the resource.                                                                                   |

|                             |                                                                                                                                                                                                                                                  |
|-----------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>restore</b>              | To retrieve individual data files from backup media and copy the files to a client without applying transaction logs. <a href="#">See recover</a>                                                                                                |
| <b>retention policy</b>     | 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. <a href="#">See browse policy</a> |
| <b>retrieve</b>             | To locate and recover archived files and directories.                                                                                                                                                                                            |
| <b>retry mechanism</b>      | Action that NetWorker software performs when client operations fail. This situation might occur because the rate of transmission is either low or undetectable.                                                                                  |
| <b>role</b>                 | Grant of user privileges to the Console. There are three roles: Console Application Administrator, Console Security administrator, and the Console User. <a href="#">See user groups</a>                                                         |
| <b>roll forward</b>         | To apply transactional logs to a recovered database to restore it to a state that is consistent with a given point-in-time.                                                                                                                      |
| <b>rollover</b>             | Backup of a snapshot to conventional storage media, such as disk or tape. Previously known as a live backup.                                                                                                                                     |
| <b>rollover-only backup</b> | Rollover whereupon the snapshot copy is deleted. Previously known as a live backup or nonpersistent backup.                                                                                                                                      |
| <b>root</b>                 | <ol style="list-style-type: none"> <li>(UNIX only) UNIX superuser account.</li> <li>(Microsoft Windows and UNIX) Highest level of the system directory structure.</li> </ol>                                                                     |

## S

|                               |                                                                                                                                                                                                                                   |
|-------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>salted hash</b>            | Added string of random data that provides a unique identifier to a user's password. <a href="#">See hash</a>                                                                                                                      |
| <b>save</b>                   | NetWorker command that backs up client files to backup media volumes and makes data entries in the online index.                                                                                                                  |
| <b>save set</b>               | <ol style="list-style-type: none"> <li>Group of tiles or a file system copied to storage media by a backup or snapshot rollover operation.</li> <li>NetWorker media database record for a specific backup or rollover.</li> </ol> |
| <b>save set consolidation</b> | Process that performs a level 1 backup and merges it with the last full backup of a save set to create a new full backup.                                                                                                         |
| <b>save set ID (ssid)</b>     | Internal identification number assigned to a save set.                                                                                                                                                                            |
| <b>save set recover</b>       | To recover data by specifying save sets rather than by browsing and selecting files or directories.                                                                                                                               |
| <b>save set status</b>        | Attribute that indicates whether a save set was successfully backed up and whether it is currently browsable, recoverable, or recyclable.                                                                                         |
| <b>save stream</b>            | Data and save set information that is written to a storage volume during a backup. A save stream originates from a single save set.                                                                                               |

|                                                  |                                                                                                                                                                                                                                                                   |
|--------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>scanner</b>                                   | NetWorker command used to read a backup volume when the online indexes are not available.                                                                                                                                                                         |
| <b>scheduled backup</b>                          | 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.                                                                                     |
| <b>secondary storage</b>                         | <a href="#">See conventional storage</a>                                                                                                                                                                                                                          |
| <b>security event</b>                            | Operation related to authorization, authentication, or configuration.                                                                                                                                                                                             |
| <b>server index</b>                              | <a href="#">See client file index</a>                                                                                                                                                                                                                             |
| <b>service port</b>                              | Port used to listen for backup and recover requests from clients through a firewall.                                                                                                                                                                              |
| <b>shadow copy</b>                               | Temporary, point-in-time copy of a volume created using VSS technology. <a href="#">See Volume Shadow Copy Service (VSS)</a>                                                                                                                                      |
| <b>shared disk</b>                               | Storage disk that is connected to multiple nodes in a cluster.                                                                                                                                                                                                    |
| <b>shell prompt</b>                              | Cursor in a shell window where commands are typed.                                                                                                                                                                                                                |
| <b>silo</b>                                      | Repository for holding hundreds or thousands of volumes. Silo volumes are identified by bar codes, not by slot numbers.                                                                                                                                           |
| <b>simple network management protocol (SNMP)</b> | Protocol used to send messages to the administrator about NetWorker events.                                                                                                                                                                                       |
| <b>skip</b>                                      | Backup level in which designated files are not backed up. <a href="#">See level</a>                                                                                                                                                                               |
| <b>Smart Media</b>                               | EMC software application that manages media resources within a distributed environment.                                                                                                                                                                           |
| <b>snapshot</b>                                  | <a href="#">See snapshot save set</a>                                                                                                                                                                                                                             |
| <b>snapshot</b>                                  | 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. |
| <b>snapshot policy</b>                           | 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.                                              |
| <b>snapshot save set</b>                         | Group of files or other data included in a single snapshot. Previously called a snapset.                                                                                                                                                                          |
| <b>snapup</b>                                    | Term previously used by Avamar software to refer to backup.                                                                                                                                                                                                       |
| <b>stage</b>                                     | To move data from one storage medium to a less costly medium, and later removing the data from its original location.                                                                                                                                             |
| <b>stand-alone</b>                               | In a cluster environment, a NetWorker server that starts in noncluster (stand-alone) mode.                                                                                                                                                                        |
| <b>stand-alone device</b>                        | Storage device that contains a single drive for backing up data. Stand-alone devices cannot automatically load backup volumes.                                                                                                                                    |
| <b>STL</b>                                       | Silo Tape Library.                                                                                                                                                                                                                                                |

|                              |                                                                                                                                                                                                                                                   |
|------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>storage node</b>          | 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. |
| <b>synthetic full backup</b> | Backup that combines a full backup and its subsequent incremental backups to form a new full backup. Synthetic full backups are treated the same as ordinary full backups.                                                                        |

## T

|                                                                   |                                                                                                                                                                          |
|-------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>tape service</b>                                               | NDMP DSP service that controls access to tape storage. A system can simultaneously host multiple tape services corresponding to multiple backup streams.                 |
| <b>target client</b>                                              | 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. |
| <b>target database</b>                                            | Database that the NetWorker server backs up as a safeguard against data loss.                                                                                            |
| <b>target sessions</b>                                            | The number of simultaneous backup data streams accepted by a backup device.                                                                                              |
| <b>temporary enabler</b>                                          | Code that enables operation of the software for an additional period of time beyond the evaluation period. <a href="#">See enabler code</a>                              |
| <b>transaction log</b>                                            | Record of named database transactions or list of changed files in a database, stored in a log file to execute quick restore and rollback transactions.                   |
| <b>transmission control protocol / internet protocol (TCP/IP)</b> | Standard set of communication protocols that connects hosts on the Internet.                                                                                             |
| <b>trap</b>                                                       | Setting in an SNMP event management system to report errors or status messages.                                                                                          |

## U

|                            |                                                                                                                                                                                                                          |
|----------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>update enabler</b>      | Code that updates software from a previous release. It expires after a fixed period of time.                                                                                                                             |
| <b>user</b>                | <ol style="list-style-type: none"> <li>1. A NetWorker user who can back up and recover files from a computer.</li> <li>2. A Console user who has standard access privileges to the Console server.</li> </ol>            |
| <b>user alias</b>          | Username seen by the NetWorker server when a Console user connects to the NetWorker server.                                                                                                                              |
| <b>user authentication</b> | Feature that validates user sign-on attempts. NetWorker can validate sign-on attempts against either a central authority, such as an LDAP database, or a local Console database. <a href="#">See host authentication</a> |
| <b>user data</b>           | Data that is generated by users, typically for the purposes of a business function. A Microsoft Word document or an Excel spreadsheet is an example of user data.                                                        |
| <b>user groups</b>         | Feature that assigns user privileges. <a href="#">See role</a>                                                                                                                                                           |

## V

|                                         |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              |
|-----------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>versions</b>                         | Date-stamped collection of available backups for any single file.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |
| <b>virtual cluster client</b>           | NetWorker client that is not permanently bound to one physical host but is managed by a cluster manager. It is also referred to as a logical cluster client or a virtual client.                                                                                                                                                                                                                                                                                                                                                                             |
| <b>virtual server</b>                   | <ol style="list-style-type: none"> <li>1. Server, usually a web server, that shares resources with other virtual servers on the same computer to provide low-cost hosting services.</li> <li>2. In a cluster configuration, a set of two nodes, which are physical computers, and virtual servers. Each node and virtual server has its own IP address and network name. Each virtual server also owns a subset of shared cluster disks and is responsible for starting cluster applications that can fail over from one cluster node to another.</li> </ol> |
| <b>virtual tape library (VTL)</b>       | Software emulation of a physical tape library storage system.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                |
| <b>volume</b>                           | Identifiable unit of physical storage medium, such as magnetic tape or disk file system used to store data.                                                                                                                                                                                                                                                                                                                                                                                                                                                  |
| <b>volume ID (volid)</b>                | Internal identification that NetWorker software assigns to a backup volume.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |
| <b>volume mount point</b>               | Disk volume that is added into the namespace of a host disk volume. This allows multiple disk volumes to be linked into a single directory tree, and a single disk or partition to be linked to more than one directory tree.                                                                                                                                                                                                                                                                                                                                |
| <b>volume name</b>                      | Name that you assign to a backup volume when it is labeled. See <a href="#">label</a>                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |
| <b>Volume Shadow Copy Service (VSS)</b> | Microsoft technology that creates a point-in-time snapshot of a disk volume. 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                                                                                                                                                                                                                                                                                                 |
| <b>VSS component</b>                    | A subordinate unit of a writer. See <a href="#">writer</a>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   |

## W

|                                  |                                                                                                                                                                                                                                               |
|----------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Windows disaster recovery</b> | Bare metal recovery of a host. NetWorker provides an automated bare metal recovery solution for Windows.                                                                                                                                      |
| <b>writer</b>                    | Database, system service, or application code that works with VSS to provide metadata about what to back up and how to handle VSS components and applications during backup and restore. See <a href="#">Volume Shadow Copy Service (VSS)</a> |

## Glossary

# INDEX

64-bit Windows operating system 617

## A

aborting a recover 686

ACPI

NetWorker support 720

OnNow 720

recover considerations 720

scheduled backup considerations 720

actions, notifications 452

Active Directory

backup 718

domain controller 718

explained 718

recover 718

SYSTEM STATE save set 718

adding

annotation 426, 427

enabler code 477

folder 483

host 482

license 477

multiple hosts 485

addresses

server, changing 699

administration window

opening 41

Administration window 38

administrators

group 45

Advanced Configuration and Power Interface. See ACPI

720

Advanced File Type Device

concurrent access 171

notification 168

retention policy 168

simultaneous recovery of save sets 171

aes encrypted data

implementing 102

recovering 367

AFTD load balancing 170

alert priority 425, 436, 440

alerts

lists priority, category, time, and message 430

Alias attribute 697

aliases, host sharing restriction 684

annotation

adding 426, 427

attribute 424

icon 426

viewing 426, 427

application specific module (ASM) 278

archive

changing time of 313

request, starting automatically later 442

stopping request in progress 442

Archive attribute 268

Archive button 46

archiving

archive pools

errors 701

archive requests

creating 311

defined 311

deleting 313

disabling 316

editing 313

archive services

enabling 310

archive volume pool 306

compared to backups 306

copying an archive request 312

disable scheduled archive 442

enabling 308

grooming files 306

indexed 307

licensing 306

managing 316

manual 310

naming archive requests, errors 701

NetWorker User program

toolbar function 46

nonindexed 308

nsrarchive program considerations 701

permissions 308

pools

configuration 289

creating 298

types of pools 309

remote requests, failure 701

requesting an archive 441

requesting an archive's status 430

requirements 306

retrieving from client machine 313

save sets

multiple 701

retrieving 314, 315

scheduled 311

scheduling 316

starting 316

stopping 316

time change 313

tracking entries 306

troubleshooting 700

viewing details 316

volumes, cloning 334

ASM (application specific module) 278

attribute

annotation 424

auth code 477

- category 424
  - enabler code 477
  - Grooming
    - limitation 311
  - message 424
  - note 424
  - priority of managed event 424
  - See also specific attribute name 690
  - server name 424
  - time 424
  - auth code attribute 477
  - authentication
    - nsrauth 531
    - oldauth 531
  - authorization code
    - error message 703
  - Auto Media Management
    - recyclable volumes 234
  - auto media verification
    - media position errors 682
  - Autochanger parallelism 493
  - autochangers
    - AIX considerations 732
    - attributes
      - new 690
    - autodetection 691
    - control ports access 693
    - destination component 691
    - HP-UX considerations 731
    - installation, HP-UX considerations 728
    - maintenance commands 691
    - STK-9840 732
  - Autorestart attribute 246
  - Autostart attribute 246
- B**
- back ups, manual 105
  - backing up Console 104
  - backing up renamed directories 65, 121
  - Backup button 46
  - backup configuration wizard 61
  - backup groups. See groups 244
  - backup levels
    - 1-9 263
    - described 263
    - options 263
    - overriding 263
    - planning 264
    - types
      - consolidated 259, 260, 263, 266
      - full 263, 266, 684
      - incremental 263
      - level 266
      - skip 263
    - usage 266
  - backup schedules. See schedules 256
  - backups
    - adhoc 51
    - Backup and Recover Server service 526
    - balancing resources 244, 259
    - bootstrap 254
    - client-initiated 289
    - commands
      - example 113
      - savepnpc program 117
    - completed 254
    - consolidated 259, 260
    - customization scripts 112
    - cycle, using levels 258
    - directives 270
    - failed 110
    - filesystems 260
    - force incremental 251
    - groups. See groups 244
    - hard links 110
    - incremental
      - pool for 288
    - large client filesystems 532
    - large filesystems 260
    - levels 266
    - log file 110
    - manual
      - policies 240
      - pool for 289
    - NetWorker User program
      - browse windows 46
    - nonscheduled 51, 60, 71
    - operations
      - stopping 681
    - operators group 45, 526
    - permissions, backup operators group 526
    - pools 284
    - previewing 253
    - recoveries 679
    - save sets. See save sets 532
    - server, forced 687
    - time intervals, setting 251
    - troubleshooting 679
    - types of backups. See backup levels 266
  - bar chart 401
  - basic reports 394
  - best practices for cloud backups 174
  - BMR support
    - recovery process 367
  - bootstrap
    - emailing 254
    - pools 286
    - printing
      - failure 687
  - browse policies
    - about 232
    - client file index growth 510
    - clones, storage nodes 335
    - defined 232
    - save set recoveries 370, 374
    - usage 232
  - browse windows
    - described 46
    - toolbar 46
  - browser
    - unresponsive 703

**C**

capture of managed event 424  
 case sensitivity 419, 473  
 category attribute of managed event 424  
 centralized  
     license management 37  
 changing  
     name of folder 484  
 changing servers 47  
 characters  
     illegal 483, 484  
 characters, not permitted 483, 484, 496  
 chart formats 398  
 checkpoint restart backups 92  
 CHKDSK, running 71  
 client  
     Sun StorageTek EBS  
         definition of 528  
 client alias, changing 684  
 client backup configuration wizard 61  
 Client Direct 35, 65, 92, 152, 153, 165  
 client file index  
     backup level, pool for 288  
     browse policies 232, 516  
     checking 686  
     clones and storage nodes 335  
     cross-checking 513  
     defined 510  
     entries  
         removing 516, 517  
     growth 510  
     location, designating 514  
     managing size 516  
     operations  
         checking 511  
         moving 514  
         recovery 351  
     policies 516  
     pools 286  
     save sets  
         cycles, removing 517  
         entries 234  
         removing 516  
     size  
         management 516  
         notification 686  
 Client parallelism 491  
 Client Retries attribute 246  
 client-initiated backups  
     pool for 289  
 clients  
     aliases, problems 684  
     backup commands 112  
     cloning  
         examples 327  
     configuration 528  
     defined 528  
     DHCP 526  
     DNS name resolution 526  
     editing 528  
     groups 244  
     large filesystems 260

manual backups 60  
 multiple 531  
 NetWorker User program 45  
 operations  
     archive retrieve 313  
     backing up renamed clients 685  
     backups 532  
     creating 528  
     editing 528, 529  
     indexes, moving 514  
     installation 528  
     manual backups 60  
     recovery, failure 685  
 policies, multiple 237  
 priority 533  
 save sets 532  
     Solaris binary location 726  
 clone pools, configuring 289  
 Clone reports 392, 408  
 Clone Volumes dialog box 329  
 cloning  
     archives 334  
     defined 320  
     destination volume, defined 320  
     examples 327  
     manual 325  
     online indexes, storage nodes 335  
     recovery  
         save sets 329  
         volumes 329  
 save sets  
     manually 327  
     performing 325  
 source volume, defined 320  
 storage nodes  
     online indexes 335  
 volumes  
     creating 329  
     details, viewing 329  
     process 329  
 cloning to cloud 178  
 cloud  
     best practices 174  
     cloning 178  
     compared to other device types 173  
     data consumption information 178  
     prerequisites 174  
     reports 416  
     setting up a cloud device 175  
     staging 178  
     support for 173  
 Cluster services 619  
 command  
     gst 55  
     savepsm 104  
 command line  
     reporting 394, 421, 422  
     reporting program 422  
 completion data retention 391  
 Completion Data Retention 391  
 completion message retention 391  
 compression, data 103

configuring  
 Host reports 415  
 reports 395  
 Sun StorageTek EBS Backup Statistics reports 404, 409, 412

connection  
 problem 703  
 refused 703

Console  
 environment variables 470

Console client  
 starting, after the first time 40

Console software  
 HTTP service port 39  
 improving performance 470  
 License Manager 478  
 managing window 37  
 URL 39

console window 37

consolidated backups 266

contacting server, problem with 703

Content Index Server  
 backing up 108  
 backup 108  
 defined 108  
 recover 108  
 SYSTEM DB save set 108

control zone 480

copying host 482

corrupted database 703

creating  
 folder 483  
 host 482  
 label templates 302  
 pools 290  
 staging policies 342

criteria for organizing hosts 480

critical priority 425, 436, 440

cross-checking online indexes 513

cross-platform  
 name resolution 526

CSV 420, 617

cutting and pasting host 483

**D**

daemon log file 523  
 daemon.log 523

data  
 compression 103  
 encryption with aes ASM 102  
 life cycle  
 cloned data 328  
 managing 236  
 sorting  
 into pools 285, 287, 288  
 to storage devices 289  
 verify 73

data compression 692

data deduplication 623

Data Domain deduplication 35

Data Retention dialog box 392

database  
 backing up 104  
 corrupted 703  
 corruption 703  
 delete failed 703  
 failed to store 703  
 fetch operation 703  
 database, fetch operation failure 703

db-output 706

dbsrvr9 707

dbstop output 706

DD Boost 35, 152, 153, 324

debug level 473

debug messages  
 logging stopped 703

deduplication  
 Data Domain 35

deduplication backups 102

default backup schedules 257

default pool 284, 288, 289

definition of  
 Sun StorageTek EBS client 528

delete operation failed 703

deleting  
 folder 483  
 host 482  
 label templates 303  
 license 477  
 managed event note 426  
 multiple hosts 485  
 note 426  
 problem 703  
 staging policies 344

device  
 disable 172  
 lists of 430  
 related messages 430

Device Access Information 160, 163, 167

Device configuration wizard 158

devices  
 device drivers  
 maintenance commands 691

device ordering  
 correcting device order problems 189  
 detecting device order problems 188

disk label errors 687

filesystem  
 staging 342  
 labeling errors 687  
 load balancing 170  
 pools 289

DFS (Distributed File System)  
 junctions 712  
 recover 714

DFSR 619

DHCP (dynamic host configuration protocol)  
 clients 526

DHCP (Dynamic Host Configuration Protocol)  
 database 109, 369  
 static IP address for NetWorker server 699

dialog box  
 Data Retention 392

directed recovery  
 access 348  
 advantages 348  
 defined 348  
 use of 348

directives  
 ASM (application specific modules) 278  
 copying 271  
 creating 270  
 defined 270  
 deleting 271  
 editing 271  
 naming restrictions 683  
 preconfigured 274

disabling  
 managed event capture 424

disallowed characters 483, 484, 496

disappearing managed event 427, 703

disaster recovery 376

disk space  
 insufficient 703

disk space, gstd log file 707

disk space, gstd.log 473

diskshadow 615

display problem 703

displaying  
 annotation 426, 427  
 reports 398

distributed segment processing (DSP) 152

DNS  
 hostname alias, troubleshooting 684

DNS (Domain Name System)  
 host name determination 526

document view 401

domain controller  
 Active Directory, configured by 718  
 defined 718  
 encryption keys  
 not supported 718

drag-and-drop, column 41

drill-down reports, Managed Event 413

DSA  
 DSA and NDMP Tape Server distinctions 552

duplicating host 482

dynamic addressing 526

**E**

editing  
 clients 528  
 folder 484  
 label templates 302  
 pools 297  
 staging policies 344

emailing the bootstrap report 254

emergency priority 425, 436, 440

enabler code 477

enabler code, entering 477

enabler code, problem 703

enabling  
 debug information 473  
 software 477

encrypting data  
 aes 102

Encrypting File System  
 backup 718  
 directed recover 718  
 encryption keys 718  
 explained 718  
 recover 718

entering  
 enabler code 477  
 license 477

enterprise  
 button 37

enterprise hierarchy  
 adding folder 483  
 adding host 482  
 copying folder 484  
 copying host 482  
 deleting folder 483  
 deleting host 482  
 folder 480  
 host 480  
 managing host 481  
 managing multiple hosts 485  
 moving folder 484  
 moving host 483  
 renaming folder 484  
 viewing 481

Enterprise Summary report 415

environment variable  
 GST\_DEBUG 707  
 GST\_MAXLOGSIZE 707  
 GST\_MAXLOGVERS 707  
 setting 473

environment variables  
 NSR\_DEV\_BLOCK\_SIZE\_MEDIA\_TYPE 183, 185  
 NSR\_DEV\_LOAD\_POLL\_INTERVAL\_MEDIA\_TYPE 186  
 NSR\_DEV\_LOAD\_TIME\_MEDIA\_TYPE 186  
 NSR\_DEV\_LOAD\_TRY\_TIMEOUT\_MEDIA\_TYPE 186  
 NSR\_DEV\_TAPE\_FILE\_SIZE\_MEDIA\_TYPE 186  
 NSR\_DEV\_DEFAULT\_CAPACITY\_MEDIA\_TYPE 186

error  
 database store 703

error messages  
 copy violation 687  
 destination component 691  
 disk label 687  
 environmental variables 702  
 illegal record size 682  
 media verification 682  
 print server 453  
 RPC errors 700  
 save sets 684  
 server, unavailable 700

event logs  
 backup 719  
 explained 719  
 recover 719

Event Time 413

Event Viewer 455

example  
 organizing hosts 480

sorting managed event 41  
 export formats 420  
 exporting  
     non-ASCII characters 421  
     reports 421

**F**  
 failed  
     operation 703  
 failed operation 703  
 fetch operation 703  
 file conversion, sparse to fully-allocated 688  
 file handling  
     indicators 46  
 file index missing, message 685  
 File Manager 684  
 File Replication Service  
     backup 719  
 filemarks 692  
 files  
     compressing 103  
     encrypting 102  
     HOSTS 526  
     log 706  
     open files, backing up 255  
     servers 697  
     verify 73  
 filesystem devices 342  
 filesystems  
     backups, large 532  
 firmware, verification 695  
 folder  
     adding 483  
     deleting 483  
     editing 484  
 force incremental attribute 251  
 Force Incremental attribute 261  
 formats  
     export 420  
 full backups 266

**G**  
 grooming  
     limitation 311  
 grooming files 306  
 group  
     backup, stopping 434  
     restarting backup 434  
     start immediately 433  
     viewing control details 434, 439  
     viewing status 430  
 Group resource 244  
 groups  
     attributes 246  
     backup operators 526  
     backups  
         previewing 253  
     bootstrap 254  
     client policies, multiple 237  
     completed 254  
     containing bootstrap 683

defined 244  
 filesystems, large 260  
 force incremental, setting 251  
 listing of per server 430  
 naming restrictions 683  
 NetWorker User program privileges 45  
 operations  
     copying 250  
     previewing 253  
     time intervals, setting 251  
     types 246  
 gst command 55  
 GST server process 707  
 GST\_DEBUG 707  
 GST\_MAXLOGSIZE 707  
 GST\_MAXLOGVERS 707  
 gstd  
     log 473, 707  
     process 55  
     size of log 473, 707  
 gstd log file 707  
 gstd service 54  
 gstdmodconf command 485

**H**  
 hard links, backup and recovery 110  
 host  
     adding 482  
     copying 482  
     deleting 482  
     managing 481  
     moving 483  
     organization of 480  
     transfer affidavit 468  
 Host List 415  
 host name determination  
     DHCP clients 526  
     TCP/IP 526  
 Host Reports  
     types and their configuration 415  
 hostname alias 684  
 hostname file 485  
 HOSTS file 526  
 HP-UX  
     creating device files 729  
     installing autochangers 728  
     pass-through drivers 729  
 HTML 420  
 hung browser 703

**I**  
 icon  
     annotation 426  
     priority 425  
 IIS (Internet Information Server)  
     defined 719  
 Immediate cloning 324  
 Inactivity Timeout attribute 246  
 incremental backups  
     pool for 288  
 Index Save Sets dialog box 512

indexed archives 307  
 individual user authentication 472  
 info priority 425, 436, 440  
 information, sorting table 41  
 install log 707  
 Interactive view 398  
 Internet Information Server See IIS 719  
 Interval attribute 246  
 Invalid Object id, error message 703  
 ioscan program 728

**J**  
 Java Runtime Environment 422  
 jbconfig program  
     autochangers  
         HP-UX 731  
         hanging 691  
 jobsd service 54  
 JRE 39, 422  
 Jukebox parallelism 493

**L**  
 label templates  
     attributes 299  
     components 301  
     creating 302  
     deleting 303  
     editing 302  
     naming restrictions 683  
     naming strategies 301  
     number sequences 299  
     preconfigured 299  
 labeling  
     tips 301  
 labels  
     silos, volumes 298  
 launch button 39  
 level of debug 473  
 Library parallelism 493  
 license  
     adding 477  
     deleting 477  
 License allocation failed, error 703  
 License Manager 478  
 licensing  
     archiving 306  
     copy violation 687  
     License Manager 478  
 List Report, User 415  
 LMHOSTS 526  
 load balancing 170  
 localized environments 396  
 location of  
     gst command 55  
 lockbox for pass phrases 531  
 log file 706, 707  
 log files  
     backup/recovery attempts 110  
     cloning information 320  
 logging, events 455  
 login

name 496  
 password 496  
 lsdev program 730

**M**  
 managed application 480  
 managed event  
     define 423  
     deleting note 426  
     disabling capture of 424  
     disappearing 427, 703  
     priority 425  
     sorting example 41  
 Managed Event configuration  
     parameters 413  
 Managed Event drill-down reports 413  
 Managed Event Reports 392  
 Managed Events button 38  
 managed node  
     adding 482  
     copying 482  
     deleting 482  
     moving 483  
 managing  
     host 481  
     license 478  
 manual backups 105  
 manual backups. See backups, manual 60  
 Max active devices 492  
 Max parallelism, media libraries 493  
 Max parallelism, pools 494  
 max sessions 165  
 Max sessions 494  
 Max Sessions 158  
 media database  
     cloned data 328  
     clones and storage nodes 335  
     compression 516, 519  
     cross-checking 513  
     entries, removing 517  
     managing size 510, 516  
     restoration 374  
     retention policies 232  
     save sets, entries 234  
 Media Library parallelism 493  
 media pools. See pools 284  
 media position errors 682  
 memory requirements for AFTDs 158  
 message attribute of managed event 424  
 message logs  
     failed backup/recovery attempts 110  
 message retention 391  
 messages file  
     Event Viewer 455  
 Microsoft Windows  
     backup operators group 526  
     Event Viewer 455  
 mminfo program  
     reports 241  
 moving host 483  
 multiple hosts

adding or deleting 485  
 multiplexing  
     performance issues 35  
 Multiplexing 493

**N**

name  
     folder, editing of 484  
     resolution cross-platform 526  
 naming restrictions 683  
 NDMP (Network Data Management Protocol)  
     configuration  
         options 552  
 Nested Mountpoints 368  
 NetWorker  
     startup commands 679  
 NetWorker Management Console See Console 34  
 NetWorker User program  
     adhoc backups 51  
     browse windows 46  
     changing servers 47  
     compression 103, 104  
     connecting to a server 47  
     encryption 104  
     manual backups 71  
     overview 45  
     password protection 104  
     privileges 45  
     server connection 47  
     starting 45  
     toolbar 46  
 NMC See Console 34  
 node  
     adding 482  
     copying 482  
     deleting 482  
     managed 480  
     moving 483  
 nonindexed  
     archives 308  
 note  
     attribute 424  
     deleting from managed event 426  
 notifications  
     defined 445  
     deleting 457  
     operations  
         customizing 450  
     preconfigured 446  
     printing 453  
     priorities 455  
     programs 452  
     SNMP  
         configuring 598  
         creating 600  
         modifying 599  
         nsrtrap 598  
 nsr\_avoid\_archive 614  
 nsr\_getdate program 240, 241  
 nsradmin program  
     editing the nsrla.res database 530

starting 48  
 nsrarchive program 306  
 nsrauth authentication 531  
 nsrd service 52  
 nsreexecd 55  
 nsrexecd service 53  
 nsrindexd service 52  
 nsrjb program  
     troubleshooting, HP-UX 731  
 nsrla.res database 530  
 nsrlpr program 453  
 nsrmm program 241, 516, 682  
 nsrmm daemon  
     NDMP  
         unsupported options 560  
 nsrmmdbd service 52  
 nsrmmgd service 52  
 nsrtrap  
     command line options 598  
     verbose mode 598  
 numeric order 41  
 nwrecover program  
     browse policy 232

**O**

object, reference 703  
 oldauth authentication 531  
 online indexes  
     cross-checking 513  
 entries  
     checking 511, 686  
     removing 517  
 information  
     refreshing 514  
 management  
     manual 510  
     size 515  
 moving 514  
 recovery  
     location 683  
 restoration 370  
 save sets, viewing 512  
 size considerations 510  
 volumes  
     removing 517

OnNow

Advanced Configuration and Power Interface (ACPI)  
     720  
 recover considerations 720  
 scheduled backup considerations 720  
 open files, backing up with VSS 256  
 operation failed 703  
 optimizing Console 470  
 organizational criteria 480  
 organizational structure, labeling for 301  
 organizing  
     Sun StorageTek EBS Servers  
         example 480  
 out of memory 703

**P**

page cannot be displayed 703  
 Parallel save streams 89  
 parallelism  
     performance 35  
 Parallelism 490  
 pathname restrictions 684  
 PDF report format 420  
 performance  
     features 35  
 performance of Console software 470  
 permissions  
     Archive feature 308  
     backup operators group 526  
 Persistent binding 188  
 Persistent naming 188  
 pie chart 401  
 pie report format 401  
 plot chart 401  
 policies  
     backups, manual 240  
     browse  
         about 232  
         data life cycle 236  
         defined 232  
         modifying 241  
         usage 232  
     clients 237  
     data life cycle 236  
     multiple 237  
     naming restrictions 683  
     overriding 240  
     planning 260  
     retention  
         about 232  
         data life cycle 236  
         defined 232  
         modifying 241  
         usage 232  
         volume relabeling 232  
     setting expiration 392  
 policy  
     deleting 238  
 pool  
     configuration 629  
     consolidated backup 286  
     copying resource 297  
 Pool parallelism 494  
 Pool Type attribute, with archive pools 309  
 pools  
     archive  
         errors 701  
     archives, creating 298  
     archiving 298  
     bootstrap 286  
     client file index 286  
     clones 289  
     configuration  
         archive 289  
         clone 289  
     creating 290  
     criteria 285, 287

data sorting 285, 288  
 default  
     clone pool 289  
 defined 284  
 devices 289, 290  
 editing 297  
 expression matching 286  
 incremental backups 288  
 manual backups 289  
 precedence 287  
 restrictions 285  
 save set consolidation 84  
 sorting data 289  
 volume labels 298  
 POSIX hard links, problems recovering 110  
 PostScript report format 420  
 Power Monitor service 720  
 precedence for pools 287  
 preconfigured notifications 456  
 priorities, notifications 455  
 priority  
     of managed event 425  
     symbol 425, 436, 440  
 Priority attribute 424  
 probe based backups 90  
 problem  
     contacting server 703  
 process, stopping and restarting 55  
 program not registered 703  
 Program not registered 703  
 Properties dialog box  
     NetWorker User program 47  
 provider 650  
 ps command 708  
 PSS 89

**R**

rearranging enterprise hierarchy 483  
 rearranging information in table 41  
 Recover button 46  
 recover program  
     media database 234  
     retention policy 234  
 recoveries  
     archives 313  
     Backup and Recover Server services 526  
     backup operators group 526  
     clients, renamed 685  
     clone volumes 329  
     directed  
         access 348  
         advantages 348  
         defined 348  
         usage 348  
     disaster-related 376  
     failed 110  
     files, finding for recovery 589  
     hard links created by POSIX 110  
     index-based  
         advantages 351  
     log file 110

NetWorker User program  
     browse windows 46  
 planning 260  
 save sets  
     client file index 370  
     media database 374  
 recovery  
     aborting 686  
 recycling. See volumes 516  
 reference object 703  
 refused connection 703  
 registering program 703  
 registry  
     backups 720  
     explained 720  
     SYSTEM STATE save set 720  
 remote access  
     recoveries 698  
 Remote Access list 698  
 remote archives, failure 701  
 removing  
     folder 483  
     host 482  
     license 477  
 renamed directories, backing up 65, 121  
 renaming folder 484  
 report  
     background processing 404  
     chart types 401  
     document mode 400  
     export formats 420  
     interactive mode 398  
     restricted views 403  
     User List 415  
 reports  
     basic and drill-down 393  
     command line reporting program 422  
     customized 394  
     daemon log file 523  
     daemon.log 523  
     date and time formats 396  
     Managed Event Drill-Down 413  
     save set policies 241  
     saved 418  
     viewing 398  
 Reports button 37, 38  
 requirements  
     NetWorker User groups 45  
 resolved events 427  
 resource  
     archive  
         changing archive time 313  
         request  
             copying 312  
             status 430  
     label template  
         copying 302  
     notification  
         copying 456  
         deleting 457  
     policy  
         deleting 238  
     pool  
         copying 297  
         directing data from consolidated backup 286  
     staging  
         copying a policy 344  
         user group  
             customizing privileges 503  
 Restart Window attribute 246  
 restrictions on pathnames 684  
 retention policies  
     about 232, 234  
     clones, storage nodes 335  
     defined 232  
     usage 232  
     volumes, relabeling 232  
 retention, completion data 391  
 retention, completion message 391  
 retention, save set 391  
 retrieval  
     troubleshooting 700  
 retrieving archives 313  
 retrieving save sets 314, 315

**S**

save program 112, 240, 241  
 save set  
     All save set 69  
 Save Set Data Retention  
     and Sun StorageTek EBS Backup Statistics Reports 404  
 Save Set Details 406  
 Save Set Name 406  
 save set retention 391  
 save sets  
     archives, retrieving 314, 315  
     backup commands 112  
     backups 532  
     client file index, entries 234  
     client priority 533  
     cloning  
         automatic 324  
         described 320  
         manually 327  
         status 325  
     consolidation  
         pools 84  
         usage 73, 74  
     defining 532  
     indexes, viewing 512  
     media database, entries 234  
     multiplexing 493  
     policies  
         modification 241  
         reports 241  
     predefined 69  
     recoveries  
         media database 374  
         online indexes 370  
     staging. See staging 342  
     status  
         clone 325

retention policy 234  
 suspected 329  
**savegroup** completion report 446  
**Savegroup parallelism** 492  
**savegrp** program  
 backup limitation 687  
**savepnp** program  
 message logging by 120  
 using with customized backup program 117  
**savepsm** 104  
**savestream** 284  
**scalability** 37  
**SCANDISK**, running 71  
**scanner** program  
 record size 682  
 recovering clone volumes 329  
 recovering save sets from volumes 236  
 retention policy 234  
 volumes, read-only 682  
**Schedule** attribute 246  
**Schedule** resource 244  
**schedules**  
 attributes 261  
 backup cycle 258  
 balancing 259  
 copying 263  
 default 257, 259  
 editing 262  
 large filesystems 260  
 load balancing 532  
 naming restrictions 683  
 overriding 263  
 planning 260  
 preconfigured 257  
 staggered 259  
 usage 256  
**scheduling** backups 104  
**SCSI** address selection for HP-UX 728  
**SCSI ID** 193  
**security**  
 lockbox for pass phrases 531  
**server**  
 problem contacting 703  
 setting up 487  
 web address 39  
**server name**  
 attribute of managed event 424  
**Server parallelism** 492  
**servers**  
 address, changing 699  
 backup  
     operators Group 526  
 DCHP 526  
 DNS name resolution 526  
 dynamic addressing 526  
 errors, binding to 700  
 file 697  
 index  
     backup, failure 687  
     management 510  
 notifications  
     priorities 455  
 service  
     gstd 54  
     jobsd 54  
     nsrd 52  
     nsrindexd 52  
     nsrmmdbd 52  
     nsrmmgd 52  
**services**  
     Backup and Recover Server 526  
     described 52  
     Power Monitor service 720  
**session management** 35  
**sessions**  
     lists of backup, recover, or browse sessions 430  
**setting**  
     data retention policies 392  
     environment variable 473  
     expiration policies 392  
**severity of managed event** 424  
**shadow copy** 650  
**Simple Network Management Protocol**. See **SNMP** 598  
**size of**  
     gstd log 707  
**sleep state**  
     defined 720  
**snapshot** 650  
**snapshot policy**  
     creating 239  
**SNMP (Simple Network Management Protocol)**  
     configuring 598, 600  
     defined 598  
     notifications  
         configuring 598  
         creating 600  
         modifying 599  
     nsrtrap 598  
     traps 598  
**Software Administration button** 37  
**Solaris**  
     troubleshooting 726  
     unsupported devices 726  
**sorting managed event, example** 41  
**sorting table** 41  
**Source Client dialog box** 363, 593  
**sparse files** 720  
**sparse files, converting** 688  
**Special Handling dialog box** 104  
**stacked bar report format** 401  
**stacking bar chart** 401  
**staging**  
     defined 342  
     filesystem devices 342  
**policies**  
     creating 342  
     deleting 344  
     editing 344  
     to cloud 178  
**Start Time** attribute 246  
**starting**  
     server process 55  
**status**  
     viewing

- group status 430
  - stopping Console server 55
  - storage nodes
    - affinity
      - problems 702
      - timeouts 702
      - troubleshooting 702
  - Storage Spaces 618
  - Store Index Entries attribute, with archive pools 309
  - storing database failed 703
  - Sun StorageTek EBS
    - server
      - organization of 480
    - Sun StorageTek EBS Backup Statistics drill-down reports 404, 409, 412
    - Sun StorageTek EBS Backup Statistics reports
      - types and their configuration 404, 409, 412
    - Sun StorageTek EBS Backup Statistics Reports 392
    - Sun StorageTek EBS Backup Status drill-down report 406
    - Sun StorageTek EBS Backup Status reports 406
    - Sun StorageTek EBS Backup Status Reports 392
    - Sun StorageTek EBS client
      - definition of 528
    - Sun StorageTek EBS DiskBackup
      - file type and advanced file type differences 153
      - notification 168
      - retention policy 168
    - Sun StorageTek EBS server
      - organizing 480
  - suspected save sets 329
  - symptom of problem 703
  - system standby 720
- T**
- tables
    - display or hide columns in 42
    - rearranging columns 41
    - sorting 41
  - target sessions 165
  - Target sessions 493
  - Target Sessions 158
  - TCP/IP
    - changing NetWorker server address 699
    - DHCP clients 526
    - host name determination 526
    - troubleshooting hostname alias problems 684
  - technical support, troubleshooting information 676
  - temporary enabler code
    - expired 703
  - temporary notes 424
  - time attribute of managed event 424
  - time range 395
  - toolbars
    - User program 46
  - tracking
    - cloned data 328
    - online index information 510
  - traps
    - categories 600
    - SNMP 598
  - troubleshooting
- aborted recover 686
  - AIX
    - STK-9840 732
  - archive pools 701
  - archive requests
    - naming 701
  - archives
    - multiple save sets 701
    - nsrarchive program 701
    - remote request failure 701
  - auto media verification 682
  - autochangers
    - AIX considerations 732
    - attributes 690
    - autodetected scsi errors 691
    - control port access 693
    - destination component 691
    - HP-UX 731
    - HP-UX considerations 731
    - maintenance 691
  - backups 679
  - backups levels 684
  - backups, stopping 681
  - bootstrap printing, failure 687
  - client file index
    - size growth 686
  - clients
    - alias 684
    - Solaris, location 726
  - daemons 679
  - devices
    - maintenance 691
    - Solaris, unsupported 726
  - disk label errors 687
  - DNS hostname alias 684
  - file conversion 688
  - firmware 695
  - hosts table 659
  - HP-UX
    - SCSI pass-through driver 731
    - unloading drives 731
    - unsupported media 731
  - illegal characters 683
  - licensing, copy violation 687
  - nsrexec processes 679
  - online indexes 683
  - pathname restrictions 684
  - recoveries
    - online indexes 683
    - remote access 698
  - recovering POSIX hard links 110
  - renamed client backups 685
  - retrievals 700
  - routers 695
  - scanner program 682
  - server errors, binding to 700
  - server index 687
  - Solaris 726
  - storage nodes 702
  - technical support information 676

**U**

uasm program 683  
UEFI 617  
unresponsive browser 703  
URL  
    Console software 39  
user  
    authentication 472  
    deleted 419  
user defined directives 622  
user interface  
    setting preferences 45  
User List Report 415  
user privileges 45  
User Reports 392

**V**

vanishing managed event 703  
variable  
    case sensitivity 473  
    for gstd log 707  
    GST\_DEBUG 707  
    GST\_MAXLOGVERS 707  
    setting 473  
verification  
    NetWorker User program  
        browse windows 46  
    of files 73  
Verify button 46  
view  
    document view 401  
viewing  
    annotation 426, 427  
    enterprise hierarchy 481  
    reports 398  
volume pool  
    See also pools 306  
    archive 306  
    defined 284  
Volume Shadow Copy Service  
    commands 655

controlling from Administration window 653  
controlling from command-prompt 654  
overview 650  
writers 652  
volumes  
    archive 334  
    client file index  
        removing 517  
    cloning  
        archive data 334  
        creating 329  
        recovery 329  
    labeling  
        maximum size 301  
        tips 301  
    modes  
        types 208  
    recycling 516  
    relabeling 206  
    removing 516  
    verify 73  
VSS. See Volume Shadow Copy Service 650

**W**

waiting priority 425, 436, 440  
warning priority 425, 436, 440  
web  
    browser  
        unresponsive 703  
    Console  
        server name 39  
WINS (Windows Internet Naming Service) 526  
WINS (Windows Internet Naming Service) database 109, 369  
wizard  
    client backup configuration 61  
    device configuration 158  
writer 652

**Z**

zone, control 480

