Chapter 4  Cloning Procedures  51

Cloning data.......................................................... 52
   NetWorker release 7.6 SP1 and later.......................... 52
   NetWorker releases prior to 7.6 SP1.......................... 52
Cloning options....................................................... 52
Automated cloning.................................................... 53
   Configuring auto-clone......................................... 53
Schedule cloning..................................................... 55
   Scheduling clone operations................................. 55
   Starting scheduled clone operations manually........... 58
   Monitoring scheduled clone operations.................... 58
   Viewing the clone status of a save set.................... 59
Volume cloning....................................................... 59
Cloning a save set................................................... 59
Scripted cloning...................................................... 61
   NetWorker 7.6 Service Pack 1 enhancements............... 61
   NetWorker 7.5 enhancements................................ 61
   nsrclone option descriptions................................ 62
   Using the nsrclone options.................................. 62
   Using the nsrclone command to specify a browse and retention policy .................................................. 63
Cloning archived data............................................. 63
   Scheduling a clone session for archive data.............. 64
   Cloning an archive volume manually....................... 64
Considerations to improve cloning performance............... 64
Cloning validation.................................................. 64
Displaying the backup versions in the GUI.................... 65

Chapter 5  Recovering Data from Clones  67
FIGURES

1  Cloning example............................................................................................................23
2  Staging example............................................................................................................24
3  Browse and retention policies.......................................................................................33
4  Filesystem cloning.........................................................................................................36
5  Cloning with storage nodes..........................................................................................37
6  Storage node selection criteria for reading the clone data..............................................38
7  Auto-clone action..........................................................................................................54
8  Setting up a scheduled clone session with Diagnostic View enabled.............................55
9  Staging..........................................................................................................................88
<table>
<thead>
<tr>
<th></th>
<th>TABLES</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Revision history ................................................................................ 11</td>
</tr>
<tr>
<td>2</td>
<td>Cloning options .................................................................................. 52</td>
</tr>
<tr>
<td>3</td>
<td>Descriptions of nsrclone options ...................................................... 62</td>
</tr>
<tr>
<td>4</td>
<td>NetWorker restore scenarios .................................................................... 69</td>
</tr>
</tbody>
</table>
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 contains planning, practices, and configuration information for using the NetWorker cloning feature.

Audience
This document is part of the EMC NetWorker documentation set, and is intended for use by system administrators. It contains planning, practices, and configuration information for using the NetWorker cloning feature.

Readers of this document should be able to perform the following tasks:

- Identify the different hardware and software components that comprise the NetWorker datazone.
- Follow procedures to configure storage management operations.
- Follow guidelines to locate problems and implement solutions.

Revision history
The following table presents the revision history of this document.

<table>
<thead>
<tr>
<th>Revision</th>
<th>Date</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>01</td>
<td>January 28, 2015</td>
<td>Initial release of NetWorker 8.2 SP1</td>
</tr>
</tbody>
</table>

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. 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:

- **Italic**
  Used for full titles of publications referenced in text

- **Monospace**
  Used for:
  - System code
  - System output, such as an error message or script
  - Pathnames, file names, prompts, and syntax
  - Commands and options
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
CHAPTER 1

Introduction

This chapter contains the following topics:

- Cloning integration feature ................................................................. 16
- Staging integration feature ............................................................... 16
- Benefits of cloning and staging ......................................................... 17
- Licensing ......................................................................................... 19
- Version requirements ......................................................................... 19
- NetWorker components .................................................................... 19
- Cloning example ............................................................................... 22
- Staging data example ........................................................................ 23
Cloning integration feature

Cloning is a feature of the EMC® NetWorker® software that allows for secure offsite storage and the transfer of data from one location to another. It provides the ability to create a copy of a save set from one volume to another volume.

A NetWorker clone operation can be performed at the following levels:

- **Save set**
- **Volume**
- **Pool**

Further selection criteria can also be used to specify particular types of data or clients. Although the clone operation creates a copy of the original backup data, it is not an exact copy since only the data within the backup is an exact copy. Some metadata is changed so that the clone copy can be managed as a separate and independent copy from the original. This capability allows the clone copy to be used for subsequent operations without any dependency to the original.

Multiple clone copies can be created so that a backup can be protected against corruption, local damage, site disaster, or loss. Cloning also provides a mechanism that can be used to move data from one storage type to another. For example, for offsite storage you can move data from disk to tape.

Clone operations can be configured to be run by:

- Automatic start (auto-clone)
- A schedule
- A customized script

Information about the volumes, status, and history of cloning operations can be viewed and monitored from the NetWorker 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.

Staging integration feature

NetWorker staging is a separate process but it relies on the cloning mechanism. 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. Staging is only supported for data that resides on disk-type devices.

A save set can be staged from one disk to another as many times as required. For example, a save set can 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 can clone the tape or cloud volume.

Staging can be driven by any of the following processes:

- 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 stage 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 stopped. This ensures that after staging, only a single set of save sets exists in either the source volumes or clone volumes.

**Benefits of cloning and staging**

While there may be multiple reasons to choose to clone or stage data, in most cases it is usually driven by the following main objectives.

- Additional data protection
- Performance
- Storage optimization

A NetWorker cloning operation is performed only after a successful backup which provides the following benefits:

- Allows the backup process to complete at maximum performance without any impact to speed due to multiple write acknowledgments, delays, or retries on one or more devices. Cloning limits the impact to the client, while providing data protection as quickly as possible.
- Ensures that the backup is successful, that the data is valid, and that the clone operation will complete successfully.
- Ensures that the storage requirements have been determined and that the appropriate storage is made available.
- Allows cloning to be scheduled and prioritized outside of the backup window when resources are less constrained.
- Reduces the load on the backup infrastructure.
- Allows for recoveries to be initiated easily because the backup operation has already completed.

**Note**

You cannot use the NetWorker software to create an instant clone by writing to two devices simultaneously. This operation is also referred to as parallel cloning, twinning, or inline copy. Where parallel cloning or twinning is required, consider using the NetWorker cloning feature. Using cloning will help ensure that the initial backup completes successfully. Additional data protection can also be implemented by using the optimum devices and bandwidth available for the backup environment.

**Additional data protection**

By creating a clone of the backup data you can achieve the following two goals:

- Validate that the original backup data can be read successfully which provides additional assurance that the data can be recovered. It also validates that the media where the backup resides is intact.
- With cloning, multiple copies of the data are available. One copy can be shipped offsite for vaulting which provides faster data rates than backing up directly to tape. This copy can be made available for recovery at the original site or offsite.
Performance

Performance is one benefit of staging. Data is backed up to near-line storage which is usually a backup-to-disk. The data can then be migrated to tape later based on staging policy settings for the disk device.

Storage optimization

The storage device that is used for the initial backup is often a compromise between a number of factors which include the following.

- Location
- Availability
- Capacity
- Speed
- Cost, as a result, the backup data on the initial storage device is unlikely to be on the ideal or optimum storage for the entire duration of the data's retention period.

Cloning and staging can help to use the storage devices more effectively by moving data between different types of devices. This ability provides the following benefits:

- Backups that are stored on local tape devices can be copied to other devices in remote locations without impact to the initial backup performance.
- Backups from disk devices can be copied to tape to facilitate offsite or long term storage. By moving data from disk to tape, you can use the storage capacity more effectively. The use of a deduplicated disk allows the initial storage space to be reclaimed for new backups.

Once backups have been cloned to other storage devices, the original backups can be deleted. This allows for the following:

- New backups can be written to the disk device since the initial storage space can be reclaimed for new backups.
- Multiple service levels can be accommodated:
  - The most recent backups may remain on one storage device for fast recovery.
  - Other backups may be moved to more cost effective, slower storage for less demanding recovery needs.

Tape

Tape is still the most commonly used backup storage medium and the following issues might be encountered when using it:

- Difficulty in accessing the data
- Reliability of the tape device
- Reliability of the robotic changing mechanisms
- Requirement of a long backup window

Note

Use backup-to-disk where high performance backups are required within a short backup window. The data can be staged to tape for longer term retention.
Disk devices

Disk devices are becoming more cost effective and offer advantages when deduplicating and replicating data. However, disk devices have limited capacity and can sometimes require considerable effort.

Licensing

In most cases, the functionality used for cloning or staging is incorporated into the existing NetWorker base product and requires no additional licenses or enablers. However, there are some devices that offer additional functionality and these might require additional licenses and enablers in order for this functionality to be used for cloning or staging, or for additional capacity to be made available. To ensure that the appropriate capacity and functionality licensing is applied and enabled for the devices that are being used, refer to the *EMC NetWorker Licensing Guide*.

Version requirements

NetWorker client and servers that support cloning should meet the following version requirements:

- NetWorker server must be installed with NetWorker 7.6 Service Pack 1 (SP1) or later software.
- NetWorker Management Console (NMC) must be release 7.6 SP1 or later.

NetWorker components

The NetWorker software has a number of components that allow for flexibility in the deployment of NetWorker datazone configurations. It allows for the scaling of data and the number of clients it supports.

NetWorker server

The NetWorker server is the main component that manages the other components that comprise the backup infrastructure.

A datazone is comprised of a NetWorker server and the group of components and client data that the server manages. A customer site may have one or multiple datazones depending on the size, distribution, and departmental organization.

NetWorker clients

NetWorker clients are computers, workstations, or files servers whose data can be backed up and restored with the NetWorker software. Each NetWorker client requires that the NetWorker software be installed and that the client is configured on the NetWorker server. The software also enables interaction with the NetWorker Application Modules.

In some cases, additional software is also installed that allows for local storage devices and dedicated storage nodes.
Storage node

The NetWorker storage node is a system that has a NetWorker storage device attached and is able to store backup data.

The storage node can be one of two types:

- Shared storage node (standard)
  The shared storage node is able to receive data from multiple sources and to share its storage capabilities.

- Dedicated storage node
  A dedicated storage node is restricted or dedicated to a single client and does not allow its storage to be used by other clients. In most cases, shared storage nodes should use dedicated systems so that the IO capabilities can be fully used. However, it is possible for the storage node to reside on systems that have other duties.

  By default, the NetWorker server must be a storage node to secure its own backups. In certain small environments, you can use the NetWorker server as a shared storage node for all backup client data.

  **Note**

  Use dedicated systems for shared storage nodes and to direct all client data to the dedicated storage node.

NetWorker Management Console

NetWorker Management Console (NMC) provides the graphical user interface and services necessary to manage the administration of the NetWorker software, monitor backup and restore activities, and report backup events. This separate software package is able to communicate with the NetWorker server.

In small environments, NMC is typically installed together with the NetWorker server. For larger environments, NMC can be installed on its own or on a separate system.

With the NMC, you can configure, monitor, and report on activities in real time.

Volumes

NetWorker devices use data volumes to store and manage the backup data.

Every volume must belong to a pool which allows multiple volumes to be used. In the case of tape cartridges, this procedure ensures that the correct volume and the storage node are always used.

Pools

A pool can be used to group the backups together so that data of a similar type or profile can be stored together. For example, you can create a pool for *Sunday Full* backups.

Pools also allow data to be directed to specific storage nodes or locations which help to organize the data for optimum storage and recovery and are used during cloning sessions.
Save sets

The backup data consists of one or more save sets in a single session or thread of data that has been generated by a NetWorker client of a NetWorker module. A save set contains at least one file which is located on a NetWorker volume.

Save set attributes provide the following information:

- Where the data originated
- Type of backup the save set contains
- Type of save set it is
- Date the save set was created
- Date the save set will expire
- Date the associated index will expire (browse expiration)
- Location of the data

These attributes allow the NetWorker software to ensure that the data is managed according to the policies and configuration settings applied. You can determine the status and type of the save set.

These attributes also allow you to determine:

- What has been cloned
- What needs to be cloned
- Status of the clone operation
- Status of the backup

NetWorker repositories

NetWorker software uses two separate repositories to manage data that has been backed up by using the save command. The following repositories record metadata irrespective of NetWorker client, NetWorker module, or data type:

- Media database
- Client file index

Media database

Information on the save set is stored in the media database. This database contains all of the records for all of the save sets that are currently under the control of the NetWorker software, and that have the potential to be used for recovery purposes.

The media database provides the following information:

- Location (volume) of the save set
- Size of the save set
- Offset within the volume

The media database contains limited details on what is inside the save set. The names and attributes of the files within the save set are stored in separate client indexes.

Unlike client indexes, media database entries are relatively small and require only a small amount of space for each save set. As such, the disk space requirements for the media database are generally small and disk size is dependent on the number of volumes and save sets.
Client index

There is a separate client index repository for each unique NetWorker client configured with the NetWorker software. The client indexes contain references to the save set IDs and record each file that was included in the backup of a given NetWorker client. The entries in the client file index record the following information for filesystem backups:

- Filename
- Attributes of the file
- Location of the file within the file structure
- Position of the file within the save set

Note

For NetWorker module backups, the client file index includes metadata about the individual application objects.

As some save sets might contain many files (100,000 or more) the information stored in the client indexes can grow. This growth impacts the amount of disk space required to store them. The save set browse retention policy allows customers to manage index space for save sets.

Cloning example

In this example, three save sets are created by a backup of a client with three data drives. These save sets are stored on a volume that is accessible through Storage Node A. Once a cloning action occurs, the copies of these save sets are sent to a clone pool on Storage Node B.

The following figure illustrates a cloning environment.
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.

In the following figure, the staging action will result in the deletion of the original save sets on the Volume A1, once they had been successfully staged (cloned) to volume B1. The Xs indicate that once a successful clone copy has completed, the original save sets are deleted. This is the difference between a clone and a stage operation. The save sets appear to move from one storage to another. The resulting save set is identical to that of the first, but in a different location.
Figure 2  Staging example
CHAPTER 2
Planning and Practices

This chapter contains the following topics:

- Cloning requirements .......................................................... 26
- Cloning policy ................................................................. 26
- Consider the application ...................................................... 30
- Consider the recovery scenario ............................................ 31
- Consider the browse and retention policies .......................... 31
Cloning requirements

The following requirements apply when performing clone 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 automatically mounts the volumes required for cloning.
  - 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 NetWorker administrator. The *EMC NetWorker Administration Guide* provides detailed information.

**Note**

Only one clone of a particular save set can reside on a single volume. If three clones of the same save set are specified, the NetWorker software will ensure that each clone is written to a separate volume.

Cloning policy

Cloning data has many benefits and can be used to protect and maximize the data protection infrastructure.

The following section lists some of these benefit, describes common scenarios, and provides advice on data selection.

**Note**

Ensure that all target volumes do not already contain the same clone save sets. Volumes that contain failed clone save sets might prevent additional clone sessions from completing.

Deciding when to clone

In most situations, the backup window is limited and usually all available resources are required to secure the client data in the required time period. Adding cloning requirements to this backup window impacts the amount of resources that are available for backups. Cloning should be avoided for all but the most important data or where a dedicated cloning infrastructure is available.

The need to clone data is normally driven by a requirement for additional protection or the need to move data to a specific media type or location. In both cases, the priority is to secure the data as quickly as possible so that data protection can begin. There is a high probability that any restore request within the first 48-hours will be due to local failure or corruption and that the original backup copy is the most likely source for that recovery.

In the case of a local disaster recovery or site loss, the recovery actions and objectives are likely to be very different. Selected systems and services will be given specific priorities, recovery point objective (RPO) values, and recovery time objective (RTO) values.
The decision on when to clone depends on specific circumstances. However, in most cases the clone operation can be separated and delayed from the initial backup operation. This combined with the requirement to use infrastructure outside of the backup window allows a cloning window to be created. Most or all of the cloning operations should occur within the cloning window.

With the NetWorker 7.6 SP1 scheduled cloning feature and the `nsrclone` command, cloning can be configured and scheduled independently of the backup window. It is important that, as with backup, sufficient planning and resources are made available to allow for successful clone operations to be completed.

**Note**

Do not schedule more than 30 clone sessions to start at the same time. Scheduling 30 or more clone sessions to occur simultaneously may result in timed-out and incomplete cloning sessions.

### About clone pools

The cloning operation reads a save set from a volume within a backup pool and writes it to a target volume.

Consider the following to ensure that the clones are easy to manage:

- Ensure that target volume belongs to a clone pool.
- Ensure that the volume that is used for cloning does not already contain a copy of the save set. Only one instance of a save set can exist on the same volume or pool.

As with backup pools, there can be multiple clone pools. Clone pools can be used to sort data by type, retention period, or location.

A clone pool can also be associated with one or more devices to limit the number or type of devices that are used. By using clone pools, you can expire the original save sets and reclaim the space on the initial or primary storage device while also maintaining the data for future recoveries. This extends the retention periods within clone storage pools and devices.

Save set clones have their own retention and browse periods which allow them to be managed independently from the original backup.

**Note**

The retention policy specified in a clone pool will be overwritten if a retention policy is specified in a scheduled clone operation or through the `nsrclone` command.

### Specifying a retention policy for a clone pool

You can specify a retention policy only for cloned data in a Pool resource.

1. In the clone pool to which clone backups will be directed, click the **Configuration** tab.
2. From the **Retention policy** list, select a retention policy.
3. Click **OK**. The *EMC NetWorker Administration Guide* provides information about editing or creating a pool.

**Note**

The retention policy that is specified in a clone pool will be overridden if any retention policy is specified in a scheduled clone operation.
Save sets

NetWorker save sets have various status conditions that allow you to determine:

- Current status of the save set
- History of the save set
- Validity of the save set for recovery or clone operations

Clone attributes

Clone attributes include the following:

- Browsable: Select if the save set still has an entry in the client file index.
- Recyclable: Select if all save sets have passed both the browse and retention policy time periods. The volume might be available for automatic relabeling and overwriting provided that all of the save sets on the volume are recyclable.
- 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.
- In-progress: Select if the save set is currently in the process of being backed up.

Note

In-progress save sets cannot be cloned.

- 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.
- Suspect: Select if a previous attempt to recover the save set failed. Suspect save sets are not cloned.

The following error message appears:

```
nsrclone: skipping suspect save set <ssid> cloneid <cloneid> nsrclone: error, no complete save sets to clone.
```

Multiplexed backups

Multiplexed save sets can be cloned. Clone copies of multiplexed save sets are written as a single contiguous data stream on the target media (demultiplexed). This behavior can be an advantage since multiplex backups have a read and recovery overhead. By cloning multiplexed save sets, you remove this overhead which allows recoveries from the clone to be read faster than the original backup.

When cloning multiplex save sets, note that only one save set will be cloned to the same target at the same time. However, multiple clone sessions can be started at the same time from the same source provided that they all have separate target volumes.

Save set spanning

Some devices support save set spanning where a save set spans across multiple volumes. When a save set is selected for cloning, it might start on one volume but will continue to one or more additional volumes.

When using devices that support save set spanning, it is important to:
- Identify save sets that span multiple volumes.
- Ensure that the number of continued save sets is kept to a minimum.
- Use separate pools and larger or alternative devices.
- Use the EMC Data Domain® backup-to-disk and optimized cloning feature with Data Domain devices.
- Plan ahead to ensure that the volumes are available and that they are read in an optimum sequence. A custom, scripted solution that uses the `nsrclone` command can be created and used to manage save set spanning.

Moving from or to different devices

The devices that are used for the initial backup might not be ideal for the entire data policy. Often the devices that are used for the initial backup are chosen for their speed or cost. These devices are usually local to the clients that are being protected and are subject to the same situations or scenarios that the clients are trying to be protected from. These include, power or cooling failures or site loss through natural disaster. With NetWorker cloning, you can copy or move the data to an alternate or additional device.

When data is cloned, the data is read from the source media in its native form similar to a restore operation. Cloned data is not copied on a bit-by-bit basis. As such, data can be rewritten to another device. The destination device does not need to be the same as the source device. Cloning or moving save sets from tape to disk or from disk to Virtual Tape Library (VTL) is no different than cloning data from like devices. This allows devices to be used efficiently and effectively in the right places.

**Example**

Advanced file type device (AFTD) disk devices can be used for the initial backups because of their speed and versatility.

Tape devices can be used to clone the data. This allows for an extended retention period without increasing the disk space requirements.

The use of deduplication can also provide efficient use of storage. Cloning to or from deduplication devices can ensure that these devices are used effectively.

Considerations for scheduled clone sessions

Note the following considerations when setting up scheduled clone sessions.

**Scheduling multiple clone sessions to start at the same time**

Do not schedule more than 30 clone sessions to start at the same time. Scheduling 30 or more clone sessions to occur simultaneously may result in timed-out and incomplete cloning sessions.

**Mixing save sets from different source devices**

Consider the following:

- Clone operations that mix save sets from different source devices, such as Data Domain devices, AFTD devices, or Network Data Management Protocol (NDMP) devices, may be written to different cloning target volumes. The full set of clone volumes should be shipped offsite.

**Note**

Although this behavior is by design and is recommended as a best practice, it is possible to write all save sets in the clone operation to the same clone volume.
It is a best practice to not mix normal data and NDMP data because of the way in which the data is written to tape differs. The number of filemarks and positioning is different for NDMP data.

If the clone operation includes save sets from different devices, and you want all of the 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**

Ensure that the source clone volume is mounted prior to cloning. The source clone volume contains the copy of data that is to be cloned. The *EMC NetWorker Administration Guide* provides detailed information on how to mount a volume.

If the clone source volume is on a remote storage node and is unmounted, a regular volume clone operation will not complete successfully; even if the source volume is mounted after the clone operation attempts to start.

The `nsrclone` program will stop responding with the following message:

```
Server server_name busy, wait 30 second and retry
```

This issue does not occur when the storage node is on the NetWorker server. The storage node is not remote.

**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 user interface.

To avoid this issue, perform either of the following:

- In the Administration GUI, create scheduled clone resources.
- or

In the `nsradmin` program:

1. Create a NSR clone resource.
2. Create a corresponding NSR task resource.

You can use these resources 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

**Note**

These entries are case-sensitive.

### Consider the application

When implementing a cloning policy for backup data, consider the following:

1. What NetWorker Module was used to create the original backup.
2. Consult NetWorker Module for Databases and Applications on page 93 and the NMM documentation set for specific application data cloning considerations.

Consider the recovery scenario

When implementing a cloning policy for backup data, consider the recovery scenarios. Cloning data provides a second or alternative source for the recovery. This can protect against media loss or corruption. However, if the media is located in one of the following locations, then the second copy of the data is still vulnerable to major disasters that can impact the entire site:

- On the same tape library
- On a deduplication device within the same data center (within a Data Domain environment)
- In a safe on the site

In some cases:

- More copies may be required to ensure that all of the recovery scenarios can be accommodated while maintaining the expected return on investment. This requirement may not apply to all clients and all data or be practical. However, consider the reasons why cloning is being used to ensure that the actions that are being proposed or performed meet the requirements or expectations.
- Additional protection can also be achieved by changing the target or moving tapes to a second location once the cloning operation is complete.

Consider the browse and retention policies

The NetWorker software uses browse and retention policies and applies them to every write operation:

- The retention policy determines the length of time that the data remains available for recovery on the NetWorker media database.
- The browse policy determines how long the details of the data remain available for browsing and selection on the NetWorker client index. Both the browse and retention policies impact the amount of disk space required by the NetWorker server. The recovery procedure is likely to be different if one or both of these polices has elapsed. The browse and retention polices should be equal to or greater than the client or data requirements and allow for the expected recovery conditions.

The NetWorker software is very versatile when recovering data because of how it handles the data on the media. When determining data recovery options, consider:

- The data is written in a format that is self-describing. This allows data to be read and recovered by using different NetWorker instances or versions.
- The data remains on the media until the save set data has expired. The media is relabeled or staged in the case of an AFTD.
- Up until the point when the media is relabeled, recoveries are still possible, regardless of the browse policy, expiration status, or even if the volume is known to the NetWorker software in the media database entry.

While this versatility can be relied upon when unexpected events occur, it does not replace the requirement to plan and manage the data appropriately. Care and consideration should be given when selecting browse and retention polices.
consider the location and number of copies of volumes and save sets. This ensures that
the data is available at the most likely time by using the simplest procedures.

Browse policy

For every backup that is created by using the NetWorker software, you must assign two
policies to determine how long data should be maintained and be available after the
recovery. The most important policy from an ease of recovery perspective is the browse
policy.

The browse policy determines how long the backup will be browsable, so that the ability
to review and select data for recovery is possible. This policy determines how long index
data is maintained in the respective client index, so that a browse policy of seven days
will remove data from the client index after seven days has elapsed. This allows different
clients, different data types, and different groups of clients to have browse periods that
differ.

Once the browse policy for a save set has expired, it is possible regenerate the index for a
given save set. Restoring save sets that are not in the media database on page 80
provides details.

Note

The browse policy is limited by the retention policy. The browse period cannot exceed the
time set for retention policy.

Retention policy

As with the browse policy, the retention policy is also assigned for every NetWorker
backup, regardless of its source or type. The policy lets the NetWorker software know how
long the data within a save set is expected to be maintained for recovery.

By having separate browse and retention policies, the user is not bound by the retention
period for client index information. This is useful as the recovery of data is more likely to
occur within a short period of time from when the backup was made. However, the need
to retain the information for business or regulatory reasons is likely to exceed this period.
It is therefore possible to have a browse period which is long enough to accommodate
the most likely recovery scenario, but maintain a retention period to satisfy the business
or regulatory criteria. This approach allows the disk space required by the client index to
be maintained at a more acceptable level without the overhead of large disk space
requirements and the performance and scaling concerns that would be associated with
this.

Example

The following figure shows how browse and retention policies can be used to maintain
the data available for recovery while minimizing the disk space required for client indexes
and maximizing the storage space available. By having this cascading retention period,
you can free the space on the immediate or high performance devices, and still maintain
the recovery options from the less costly, lower performance devices.
**Figure 3** Browse and retention policies

### Client index

<table>
<thead>
<tr>
<th>SSID</th>
<th>Browse(days)</th>
</tr>
</thead>
<tbody>
<tr>
<td>SS101</td>
<td>14</td>
</tr>
<tr>
<td>SS102</td>
<td>14</td>
</tr>
<tr>
<td>SS103</td>
<td>31</td>
</tr>
<tr>
<td>SS201</td>
<td>Inherited</td>
</tr>
<tr>
<td>SS202</td>
<td>Inherited</td>
</tr>
<tr>
<td>SS301</td>
<td>Inherited</td>
</tr>
<tr>
<td>SS302</td>
<td>Inherited</td>
</tr>
</tbody>
</table>

### Media DB

<table>
<thead>
<tr>
<th>SSID</th>
<th>Retention(days)</th>
</tr>
</thead>
<tbody>
<tr>
<td>SS101</td>
<td>14</td>
</tr>
<tr>
<td>SS102</td>
<td>14</td>
</tr>
<tr>
<td>SS103</td>
<td>90</td>
</tr>
<tr>
<td>SS201</td>
<td>90</td>
</tr>
<tr>
<td>SS202</td>
<td>90</td>
</tr>
<tr>
<td>SS301</td>
<td>1095(3yr)</td>
</tr>
<tr>
<td>SS302</td>
<td>1095(3yr)</td>
</tr>
</tbody>
</table>

---

AFTD volume

Clone operation

VTL volume

Clone operation

Offsite volume

Clone operation
CHAPTER 3

Software Configuration

This chapter contains the following topics:

- Filesystem configuration ................................................................. 36
- Storage nodes ................................................................................. 37
- Cloning with EMC Avamar (deduplication node) .............................. 42
- Cloning with Data Domain (DD Boost) ............................................ 43
- Cloning with EMC Disk Library using an embedded storage node .......... 46
- Production storage node cloning of data to physical tape ................. 49
Filesystem configuration

Before you start to configure cloning, you must consider the type of data that is being cloned. This section describes a basic cloning operation that uses a standard filesystem backup where a client, pool, or volume that has one or more filesystem save sets is required to be cloned to a second device. This device is typically located in a different location.

For specific application data cloning considerations, see NetWorker Module for Databases and Applications on page 93 for more information.

The following figure illustrates the principle for all cloning operations.

Figure 4  Filesystem cloning

In this figure:

- A client performs a backup to a storage node.
- The clone operation takes the copy from the storage node or another storage node that has access to the same volumes and reads the data from the volume, storage node A.
- Data is then directed to a different device. The data can be accessed in one of three ways:
  - Through the same storage node
  - From a storage node in a different location
  - By using a different device (storage node B)
Most of the configuration principles in this section apply to all cloning operations.

## Storage nodes

When performing clone operations, you can select the storage node that is used for the source and target.

This section describes the criteria that you can use to determine:

- The storage node from which the clone data is read (read source).
- The storage node to which the clone data is written (write source).

The following figure illustrates a typical NetWorker environment where a number of storage nodes and devices are available. The ability to determine the storage node and device used for both the read and the write source of any cloning operation is an important element in configuring cloning.

**Figure 5** Cloning with storage nodes

### Determining the read and write source

Selecting the appropriate read and write sources ensures proper clone operation.

Ensure the following:

- The clone copies are created from and reside in the appropriate locations or media formats.
- The resources are available for other backup or recovery operations.

The following figure illustrates the storage node selection criteria for reading the clone data.
Criteria for reading the clone data

Use the following criteria to determine the storage node from which the clone data will be read (read source).

- 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 behaves as though the volume is not mounted.
- 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 the following criteria:
  1. Storage nodes are listed in the Recover Storage Nodes attribute of the Client resource of the NetWorker server. If this attribute is empty, the Storage Nodes attribute of the NetWorker server is used.
  2. If the requested volume is in a media library, the storage nodes on which the volume can be mounted is 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 of the storage nodes on which any device in the library is configured are 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 storage nodes that are listed in the Recover Storage Nodes attribute of the Client resource of the NetWorker server. If this attribute is empty, the Storage Nodes attribute of the NetWorker server is used.

Criteria for writing the clone

Use the following criteria to determine the storage node to which the clone data will be written (write source):

- The Clone Storage Node attribute of the read source storage node is used as the write source.
- If the read source host does not have a Client resource, the Storage Nodes attribute of the NetWorker server is used as the write source.

No matter where the cloned data is directed, the client file index and the media database entries for the cloned save sets still reside on the NetWorker server. This ensures that the browse and retention policies are handled consistently regardless of where the clone data is directed.

Directing a clone from one storage node to another storage node

Use the following procedure to direct a clone from one storage node to another storage node.

Procedure

1. In the NetWorker Administration window, ensure that Diagnostic Mode is enabled by selecting View > Diagnostic Mode from the main menu.
2. Select Devices, and then double-click Storage Nodes in the left pane.
3. Right-click the read source storage node and then select Properties. The Storage Nodes Properties window appears.
4. Select Configuration.
5. In the Clone Storage Nodes attribute, add the hostname of the storage node to which the clone data will be written.

   The first entry in the list contains the functional, enabled device that receives the cloned data from the read source storage node.
6. The Clone Storage Nodes attribute applies only to NetWorker servers and storage nodes.

   **Note**

   Leave this attribute blank for NetWorker clients that are not also NetWorker servers or storage nodes.

Directing clones from all storage nodes to a single storage node

Use the following procedure to direct a clone from one storage node to a single storage node.

Procedure

1. In the NetWorker Administration window, ensure that Diagnostic Mode is enabled by selecting View > Diagnostic Mode from the main menu.
2. Select Devices and then double-click Storage Nodes in the left pane.
3. Right-click the read source storage node and then select Properties. The Storage Nodes Properties window appears.
4. Select **Configuration**.
5. In the **Clone Storage Nodes** attribute, add the hostname of the storage node to which all cloned data is to be written.

**Criteria for recovering cloned data**

Use the following criteria to determine the storage node from which the clone data will be recovered:

- 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 behave as though the volume is not mounted.
  - When cloning is used in a VTL environment such as an EMC CLARiiON Disk Library (CDL), the NetWorker software behaves as if the FORCE_REC_AFFINITY environment variable is set to Yes.
- 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 the following criteria:
  - The storage nodes listed in the Recover Storage Nodes attribute of the NetWorker client resource that is being recovered. If this attribute is empty, the NetWorker client’s Storage Nodes attribute is used.
  - 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 are 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 storage nodes that are listed in the **Recover Storage Nodes** attribute of the Client resource of the NetWorker server. If this attribute is empty, the Storage Nodes attribute of the NetWorker server is used.

**Cloning with tape devices**

There are a number of reasons why tape devices are used as part of the cloning process.

- In cases where tape is used as a secondary storage tier where selected data is cloned to tape for offsite storage or for extended data retention periods. This allows disk devices to be used for the initial backup where their speed and flexibility can be most effectively used for fast backup and recovery performance.
- In cases where tape is used as the primary backup media, there are still benefits in creating clone copies, including:
  - Secondary copy at different location or for offsite storage
  - Data validation
  - Verification of the ability to read data from the media
  - Added protection of multiple copies across multiple volumes
  - De-multiplexing of multiplex backups for faster recovery

Cloning with tape devices provides two benefits which should be considered for every clone created:
Unlike disk-based devices, tape devices read data in a serial format. This means that while multiplexing is beneficial from a backup streaming perspective, this is not the case for recovery.

If recovery speed is important, the use of clone copies as the source is likely to result in faster recovery throughput.

Tape clone copies are often the preferred method to read data in disaster recovery situation. The ability to acquire, install, and configure a tape unit to read data is often the first task on a disaster recovery plan.

By creating a copy of the backup on tape, you can eliminate the need for appliances such as VTLs or disk systems to be in place. This often takes longer to acquire, install, and configure. However, ensure that the tape copy is a full and complete copy, without the dependence on other backups or deduplication appliances to complete the restore operation.

Cloning with file type and AFTD devices

The use of the disk backup devices such as file type and AFTD devices are ideal for cloning operations because they provide high speed, random access, and flexibility.

In many cases, the disk devices are used as the initial target device for backups, especially in situations where slower clients are unable to match the speeds expected for modern tape devices. In these situations, the ability to clone or stage data to tape often provides extended retention and data protection while maximizing the disk use and benefits.

Data can remain on the disk devices for short periods, typically 3 to 14 days, which allows for:

- Adequate time for immediate and urgent restore operations to occur.
- Plenty of time to create further copies to tape or other disk-based devices for longer term retention.

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 AFTD, automatic cloning begins only after all the save sets in a savegroup have been backed up.

**Note**

You can begin manually cloning a save set as soon as it has finished its backup.

- Beginning with release 8.0, NetWorker does not create read-only mirror devices for AFTD and DD Boost devices. NetWorker 8.0 provides both write and read functionality on existing and new devices. The NetWorker 8.0 installation removes legacy read-only mirror devices. You can also save, recover, and clone to and from the same device concurrently.
- AFTD devices allow recoveries during cloning operations (Read(source) or Write(target)). This assumes that the recover operation is not from the active save set and that only one clone operation is running at-a-time.
Manual cloning with advanced file type device

Consider 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.
- Launch the cloning process for that save set as each save set is backed up.
- Clone only one save set at a time.

Cloning with EMC Avamar (deduplication node)

EMC Avamar® deduplication technology decreases the amount of time, network bandwidth, and disk capacity required to back up client data.

The cloning of Avamar deduplication backups is somewhat different from the cloning of other NetWorker backups. Only the metadata (hash information) is stored on a NetWorker storage node. This metadata is not deduplicated. However, it can be cloned in the usual manner. Scheduling clone operations on page 55 provides information on how to set up cloning operations. Cloning this hash metadata is highly recommended.

The backed-up data from an Avamar deduplication client is stored on an Avamar deduplication node and cannot be cloned to a NetWorker storage node. This backed-up data can be replicated on another Avamar deduplication node if such a replication host has been configured. The NetWorker software does not initiate replication. A replication host (an Avamar server) must be configured by EMC Customer Support before a deduplication backup can be replicated. The EMC NetWorker Administration Guide provides more information. You can also output the backup data of Avamar deduplication nodes to tape volumes. Backup-to-tape for Avamar deduplication clients on page 42 provides more information.

Note

For disaster recovery, you must replicate the client data to another Avamar deduplication node. You must also clone the metadata. Both the metadata and the client data are required to recover backed-up client data.

Backup-to-tape for Avamar deduplication clients

There is an alternate method to using a replication node to ensure that additional copies of Avamar deduplication data are available for recovery.

Create a second instance of the client to be backed up, but do not configure the second instance as a deduplication client. The second client instance is treated as a regular NetWorker client and its data is backed up to tape.

Backing up to tape for Avamar deduplication clients

Clients Mars, Venus, and Jupiter have been configured as deduplication clients and assigned to a backup group named Dedupe backups. This group is scheduled for a daily level full backup.
Procedure

1. Create another instance of the Mars, Venus, and Jupiter clients.

   Note
   Do not select the Deduplication backup checkbox on the Apps & Modules tab of the Create Client resource.

2. On the General tab of the Create Client resource, assign Mars, Venus, and Jupiter to a backup group named Tape backups.

3. Schedule this group for a monthly full backup on one day of the month. Skip every other day of the month.

   Note
   The Avamar documentation describes the tape out options that are available for Avamar.

Cloning with Data Domain (DD Boost)

As with other NetWorker devices, Data Domain device types can also be used to perform clone operations. Single save sets or the entire volume of a Data Domain device may be cloned as a source or target.

Clone formats

Data stored on a Data Domain device may be cloned by the NetWorker software in one of two formats, depending on the type of media on which the clone copy will be stored:

- Clone-controlled replication format
- Regular clone format

Clone-controlled replication format

Data that is cloned to a target Data Domain device, typically at a remote location, retains its deduplication format and is known as clone-controlled replication (CCR) or as an optimized clone.

Clone-controlled replication uses the native Data Domain replication feature to copy data from one Data Domain system to another.

Clone-controlled replication uses a special Data Domain API command. Do not confuse this clone-controlled replication with standard directory level replication, which is also supported. The clone is created quickly and uses low bandwidth and low storage capacity.

A clone created in this format may be used for data recovery or to create further copies, for example, to traditional disk or tape storage. This method results in minimal impact on production or primary backup and recovery operations.

Immediate cloning

NetWorker 8.1 and higher supports immediate cloning with clone-controlled replication. Immediate cloning means that each save set can be cloned after it is backed up instead of waiting until all save sets in the group are backed up before starting clone operations. Cloning operations can complete sooner because they can now run in parallel instead of sequentially. Performance gains are most noticeable when there are many savesets in the backup queue or when there are many savesets of different sizes.
Immediate cloning is set up by using the automatic savegroup cloning feature. When you select the automatic clone operation feature for a backup group resource, select the clone mode Start on each saveset completion. See Automated cloning on page 53 for more information.

Regular clone format

When data on the Data Domain device is cloned to a traditional disk or tape, it is reverted to its native non-deduplicated format, known as "regular clone" format. Regular clone format is necessary for the data on traditional disk or tape storage to be completely recoverable, for example for disaster recovery, without the need of a Data Domain system.

The process that takes data that has been deduplicated and then reverts it to normal or regular data is called rehydration.

Clone requirements

To clone data from one Data Domain device to another by NetWorker clone-controlled replication (optimized cloning), ensure that requirements are met.

The following eight requirements assume that the previous creation of a clone target pool named, newclonepool:

1. Ensure that both the source and target storage nodes are clients of the same NetWorker server.
2. Ensure that the Data Domain systems are properly licensed, including a replication license, which is required to create optimized clones.
3. Ensure that the Client resource for the NetWorker server and both storage nodes specify in their Aliases attribute all of their names in use. For example:
   - Fully-qualified name
   - Short name
   - Aliases
   - IP address

   **Note**
   If an nsrclone command or script is used to perform an optimized clone from a host that is not the NetWorker server, then this command must specify the NetWorker server by its primary hostname as listed in the NMC Enterprise view. Otherwise, a regular clone might be produced instead of an optimized clone.

4. Ensure that a target pool (for example, newclonepool) has been created for Backup Clone type with the Media type required attribute set to Data Domain. With this setting, if a Data Domain device is not available for a clone operation in the specified target pool, then NMC displays a "Media waiting" message.

   **Note**
   The Default Clone pool does not allow any modification. The required media type cannot be set in that pool.

5. Ensure that the Client resource for the source storage node specifies, in its Clone Storage Node attribute, the target storage node hostname:
• If the Clone storage node attribute is not specified, then the NetWorker server becomes the storage node for the clone operation.

• If the Clone storage node attribute lists a storage node for a volume that is not Data Domain, and media type required is not set to Data Domain in the target clone pool, then only regular clones may be stored on those volumes.

**Note**

This setting is not required if the target storage node is on the NetWorker server.

6. Ensure that the source Data Domain device is mounted and available on the source storage node. If the source device is not mounted, then a regular, non-deduplicated clone will be performed. However, if the specified target pool is of Backup Clone type with the Media type required attribute set to Data Domain a non-deduplicated clone will not be performed.

7. Ensure that the target Data Domain device is labeled and mounted on the target storage node. The pool selected for the device label operation (for example, newclonepool) must be of Backup Clone pool type.

8. Verify that the target clone pool (for example, newclonepool) is properly specified or selected:

   • For CLI clone operations, use the `nsrclone -b newclonepool` command.

   • For scheduled clone operations, in the Write clone data to pool attribute of the Clone resource, select `newclonepool`.

   • For auto-clone operations for a group, in the Clone pool attribute of the Group resource, select `newclonepool`.

   • For clones of entire volumes, Cloning by pools on page 45 provides details.

**Cloning by pools**

In order to copy save sets from Data Domain storage to a device, a special pool must be specified. This pool is known as a "clone pool." A clone pool must be assigned to a device on the target Data Domain system, where it will be available for use.

There are two main purposes for a clone pool:

• To copy existing deduplicated VTL or CIFS/NFS AFTD save sets to a Data Domain device.

• To copy the existing save sets from one Data Domain device to another Data Domain device, typically at a remote location for disaster recovery purposes.

**Parallel cloning for Data Domain CCR**

Parallel cloning is a feature of clone-controlled replication (CCR) for Data Domain systems that enables clone operations to occur concurrently, similar to parallel save set sessions. By default, NetWorker performs up to 30 parallel concurrent cloning sessions or threads from each source clone pool per CCR operation. This is the recommended setting, but it can be changed as follows:

**Note**

If you try to clone a save set that must be read from more than one source pool, then NetWorker will queue the backup pools. To avoid this, use a separate CCR operation for each pool.
Procedure

1. Create a file named nsrcloneconfig, with no file extension, in the following location on the host that runs the CCR.
   - On Microsoft Windows systems: C:\Program Files\EMC NetWorker\nsr\debug
   - On UNIX systems: /nsr/debug

2. In this file, you can type the following two global and two resource-specific parameters:
   - max_threads_per_client=
   - max_concurrent_save_sets
   - max_client_threads=
   - nsrclone_resource_name_max_threads_per_client=
   - max_concurrent_save_sets
   - nsrclone_resource_name_max_client_threads=

where:

- max concurrent save sets limits the number of parallel clone sessions that NetWorker will run on any one source client, for example, 15.
- max clients limits the number of source clients that NetWorker will include in the parallel cloning operation, for example, 2.
- nsrclone_resource_name is the name of the specific NetWorker Clone resource you will use, added as a prefix to the parameter.

The numeric values multiplied must not exceed 30 or an error message results. If you use both global and resource-specific settings, then the specific settings override the global settings. To disable parallel cloning, set both values to 0. This will result in a queue with sequential cloning only.

Cloning with EMC Disk Library using an embedded storage node

The storage node cloning capability within the EMC Disk Library® (EDL) requires a NetWorker storage node. This means that the EDL with the embedded storage node cloning capability must be configured in a NetWorker datazone. All standard NetWorker configuration rules and restrictions apply.

The embedded storage node software feature automatically starts when the EDL NetWorker Storage Node enabler license is installed. The storage node software also automatically restarts after an EDL reboot, as long as the enabler license remains installed. If the EDL NetWorker Storage Node enabler license is removed, the storage node software is stopped and will remain stopped until the EDL reboot.

Activating the EDL embedded NetWorker Storage Node enabler license also enables a menu option within the EDL Console that checks the status of the storage node and enables starting and stopping of storage node services. The EMC Disk Library online help provides more details.

Embedded storage node use cases

The embedded storage node feature supports all standard NetWorker cloning operations, including these six use cases:

1. Cloning save sets from virtual tape with the disk library to Fibre Channel-connected target libraries on the back end of a disk library:
   - The disk library embedded storage node reads save sets from the virtual tape library that are used by the production storage node, and writes to the target tape devices that are attached to the back-end Fibre Channel ports of the disk library.
• A different retention policy can be applied to the cloned copy of the save set.
• Setting different retention policies can enable the copy on the virtual media to be retained for a relatively short period of time.

2. Cloning save sets from virtual tape to a second Fibre Channel-connected disk library on the back end of the disk library. This cloning operation has the advantage of maintaining a second copy of data on disk, while freeing space on the primary backup target.

3. Cloning of save sets from virtual tape to a remote disk library through extended back-end Fibre Channel SAN connectivity:
   • This allows electronic cloning of a save set or distance, where the remote tape device is written to by the local disk library storage node.
   • Recovery of the save set can also be accomplished over that same distance if necessary.

4. Cloning of the save sets from virtual tape to a second disk library with embedded storage node over IP:
   • This provides the ability to:
     ▪ Clone over a relatively low-cost infrastructure including one that may be already be in place.
     ▪ Keep the remote data on a disk library.
   • This is particularly useful when a limited amount of data needs to be moved (1 to 2 TB per day depending on the distance).
   • Performance limitations of the existing IP infrastructure will impact the amount of data that can be cloned with this solution.

5. Cloning of the save sets from virtual tape to a different or separate NetWorker storage node over IP:
   • This provides the ability to clone over a relatively low-cost infrastructure, one that may be already in place without requiring a second disk library at the remote site.
   • This is particularly useful when a limited amount of data needs to be moved (1 to 2 TB per day depending on the distance).
   • Performance limitations of the existing IP infrastructure will impact the amount of data that can be cloned with this solution.

6. Cloning of save sets in virtual tape libraries on either disk library engine from one disk library engine addresses these points:
   • Allows a single embedded storage node to clone from VTLs in either disk library engine.
   • Allows a single embedded storage node to clone from other virtual tapes if the other disk library engine is down.

**Cloning operations with embedded storage nodes**

The environment that supports this use case provides an additional level of availability for embedded storage node cloning operations.

An embedded storage node is similar to any other storage node in that the node can use the devices that it can see such as:

• Virtual tape library on its own disk library engine.
• Target tape library (PTL) connected to the same disk library engine. However, it cannot see the virtual tape library in the other disk library engine. But it can:
- Treat engine A, which functions as a Fibre Channel initiator, as a SAN client of engine B that functions as a Fibre Channel target.
- Engine B provides the same VTL used by the production node to engine A.
- Each disk library engine becomes a SAN client of the other, just like any other SAN-connected NetWorker storage node. This requires each embedded storage node to have this capacity.

- Read from the virtual tapes that were created by the production storage nodes.
- Write to either virtual or physical tape devices that are attached to the disk library or to a second or remote storage node. The NetWorker software allows a tape library to be shared by two or more storage nodes. This can occur in two instances both of which are supported by the embedded storage node cloning capability.

In the previous scenarios, one or more virtual tape libraries were created within the disk library and assigned to the NetWorker storage nodes. These virtual tape libraries can be used by a single or multiple production storage nodes, or by the embedded storage node.

For the embedded storage node to access these virtual tape libraries for cloning operations, the virtual tape libraries must also be assigned to the NetWorker storage node which is the SAN client in the Disk Library Console program. This allows the embedded storage node to:

- Read from the virtual tapes that were created by the production storage nodes.
- Write to either virtual or physical tape devices that are attached to the disk library or to a second or remote storage node.

The NetWorker software allows a tape library to be shared by two or more storage nodes. This can occur in two instances both of which are supported by the embedded storage node cloning capability:

- Dynamic Drive Sharing (DDS), where one or more of the tape drives in a tape library are shared by two or more storage nodes.
- Without DDS, where one or more of the tape drives are dedicated (not shared) by two or more storage nodes.

Storage node selection

The purpose of the embedded disk library storage node is to provide a highly efficient cloning process. A NetWorker datazone has one NetWorker server, one or more storage nodes, and one or more clients.

Environments with multiple storage nodes

In environments with multiple storage nodes, configure the NetWorker environment so that the NetWorker software uses the disk library embedded storage node, and not the production storage nodes to perform the cloning operations.

If not properly configured, it is possible that the NetWorker software will automatically select a production storage node in place of the embedded storage node. As a result, cloning might occur between storage nodes over an IP or Ethernet connection.

Cloning node affinity for all disk library virtual tape libraries

By default, the NetWorker software determines which storage node will read a source volume in a clone operation by first considering if the source volume is already mounted.
While this is an efficient choice for many situations, it is not preferred for environments where clone operations are to be performed by the disk library embedded storage node. NetWorker version 7.4 SP1 and later incorporates a feature where the mounted status of a source volume is ignored when determining the read source for virtual tape libraries.

**Note**

Use this feature when performing any cloning operation that involves the disk library embedded storage node. This feature is applied to the NetWorker server, not the embedded storage node that is running inside the disk library.

The NetWorker software automatically activates a feature that ignores the mounted tape status when determining cloning node affinity for all disk library VTLs that have the virtual jukebox attribute set to Yes in the Jukebox resource. This same functionality is available, but not automatically enabled for all other non-VTL jukeboxes.

To enable this feature on non-VTL jukeboxes on the NetWorker server:

1. Set the environment variable FORCE_REC_AFFINITY to Yes.
2. Restart the NetWorker processes.

### Production storage node cloning of data to physical tape

This section outlines the advantages and disadvantages of cloning data to physical tapes:

- The NetWorker software can clone from virtual tape in the disk library through a production storage node to a SAN-attached tape library to produce copies of save sets. This operation is a standard NetWorker cloning procedure.
- For the disk library, a virtual tape drive works in conjunction with a SAN-attached target tape device to complete the cloning process.
- Cloning from a production storage node to a second storage node can also be performed over IP.

**Note**

Do not use a production storage node to perform cloning operations when the embedded storage node cloning capability is present.

### Advantages

The advantages of cloning data to physical tapes include the following:

- Cloning can occur with the disk libraries under NetWorker control with standard NetWorker policy support. Multiple retentions policies for different cloned copies of data can be used.
- Cloning can occur at the save set level.

**Note**

An entire save set can be cloned.

- Copying can occur from one tape type (virtual) to another tape type (target tape library), also known as tape conversion.
- Copying can occur from multiple virtual tapes to a single tape, also known as tape stacking.
Disadvantages

The disadvantages of cloning data to physical tapes include the following:

- Requires storage node licenses.
- Requires maintenance of front-end SAN infrastructure to a target tape library as well as the virtual tape library.
- Consumes SAN bandwidth as data must be from virtual tape over the SAN to a target device on the SAN.
This chapter contains the following topics:

- Cloning data ............................................................................................................. 52
- Cloning options ........................................................................................................ 52
- Automated cloning ................................................................................................. 53
- Schedule cloning ..................................................................................................... 55
- Volume cloning ......................................................................................................... 59
- Cloning a save set .................................................................................................... 59
- Scripted cloning ....................................................................................................... 61
- Cloning archived data ............................................................................................. 63
- Considerations to improve cloning performance .................................................. 64
- Cloning validation ................................................................................................... 64
- Displaying the backup versions in the GUI ............................................................ 65
Cloning data

NetWorker clone operations can be configured by using several different methods. Each method is suited to different environments and storage needs. You may need to use multiple or mixed cloning approaches to achieve the required control and flexibility.

Clone operations can be configured to be run by:

- Automatic start (auto-clone)
- A schedule
- A customized script

NetWorker release 7.6 SP1 and later

In NetWorker release 7.6 SP1 and later, a clone user interface option was introduced for scheduled clone operations, and provides the following benefits:

- Combines the flexibility of using the nsrclone command and avoids some of the performance limitations that were often associated with the legacy automatic cloning method.
- Eliminates the requirement to create scripted solutions.

NetWorker releases prior to 7.6 SP1

For NetWorker releases prior to 7.6 SP1, the following cloning options are available:

- Automated clone operations. These are linked to regular backup group operations and are enabled through the Backup Group resource.
- The nsrclone command combined with a scripted solution.

Cloning options

The following table lists the cloning options and describes how and when they are typically used.

<table>
<thead>
<tr>
<th>Cloning option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Automated</td>
<td>Automated cloning is configured through the NMC at the NetWorker group level. Cloning can be set to run immediately after the group completes or after each saveset backup completes. Automated cloning on page 53 provides details.</td>
</tr>
<tr>
<td>Scheduled</td>
<td>Scheduled cloning, introduced with NetWorker 7.6.1, overcomes limitations in group cloning by providing the ability to set clone schedules and more flexible options on save set selection and clone pools. Schedule cloning on page 55 provides details.</td>
</tr>
<tr>
<td>Volume</td>
<td>Volume cloning is performed through the NMC Media window. The clone of the individual volume runs immediately. Volume cloning on page 59 provides details.</td>
</tr>
<tr>
<td>Save Set</td>
<td>Save set cloning is performed through the NMC Media window:</td>
</tr>
</tbody>
</table>
### Automated cloning

Automated cloning is linked with a backup group. With automated group cloning, save sets can either be automatically cloned when the group is completely backed up or immediately (immediate cloning) after each save set in the group is backed up.

**Note**

The scheduled cloning GUI provides more flexibility than the automated clone option.

Immediate cloning is supported only with clone-controlled replication using DD boost devices. 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 save sets in the backup queue or when there are many save sets of different sizes.

Unless immediate cloning is used, automated cloning is best suited to smaller environments, or to a small number of clients, where the clone operations need to be completed quickly. This method ensures that the backup data is cloned as quickly as possible. However, it also means that the cloning operation is likely to interfere with the backup window and might vary in start and end times.

### Configuring auto-clone

The *EMC NetWorker Administration Guide* provides details on creating a clone pool. The following figure displays the auto-clone action when the clone is set to start on group completion. Once the backup of the three save sets has completed, the clone of the save sets automatically starts. This action provides two copies of the backup on completion of the savegroup.
A savegroup that has the auto-clone attribute enabled starts a cloning session after the backup (entire group or a save set) is complete. If the savegroup is aborted or stopped after the backup is complete, the auto-clone session does not take place and the following occurs:

- Status icon in NMC displays as successful.
- Message appears in the logs to indicate that the save set cloning session failed.

Since the group is marked as successful in NMC, the restart option is not enabled on the savegroup.

To start the savegroup again, in NMC select start on the savegroup. The backup session begins with auto-clone enabled.

**Procedure**

1. In the NetWorker Administration window, select Configuration.
2. Create a Group resource and then select Properties.
3. Specify the Clones option.
4. Select a value from the Clone mode attribute.
   - Select **Start on save set completion** to start a save set clone operation on each save set that 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.

5. Select the clone pool that will be used to direct the backup.

**Schedule cloning**

NetWorker scheduled clone operations can be configured and run in NMC according to a schedule for predetermined clients, pools, save sets, and devices.

This method is suitable for environments where copies of save sets need to be regularly provided. Such an environment is typically part of a well-defined maintenance cloning window, which runs independent of the main backup operation.

The following figure shows the schedule pane for a clone session.

**Figure 8** Setting up a scheduled clone session with Diagnostic View enabled

### Scheduling clone operations

Use the following procedure to schedule clone operations.

**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:
   a. Type a unique name to identify the scheduled clone resource.
   b. Type additional information in the **Comment** attribute, if required.

5. To override the save set’s original browse and retention policies:
   a. Select **New policies** in the **Browse** attribute.
   b. Select **New policies** in the **Retention** attribute.

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.

   The Storage node to WRITE save sets attribute is used primarily in conjunction with the Storage node to READ save sets attribute. This joint usage balances the access to storage node media across different storage nodes.

   **Note**

   If a selection is made in the **Storage node to WRITE save sets** attribute, it will override any selection that is described in **Criteria for writing the clone on page 39**.

7. To specify the storage node that will read the data during the clone operation:
   a. Select a storage node value from the **Storage node to READ save sets** attribute. This attribute is visible only when **Diagnostic mode** is selected.
   b. Ensure that the selected storage node is included in at least one of the following:
      - The Recover storage nodes or Storage nodes attribute of the NetWorker server’s Client resource.
      - A storage node list 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.

   **Note**

   The **Storage node to READ save sets** attribute is not intended for use with stand-alone devices such as AFTDs, file type devices, and Data Domain devices.

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.

   **Note**

   If no selection is made, clones will be written to the default clone pool.

9. Use the **Pool** attribute to ensure that only certain media types are used to hold clone data. Pools direct backups to specific media volumes.

   For example, to ensure that this clone session replicates only to:
   - A certain type of disk, such as a Data Domain type disk, select a clone pool that uses only Data Domain type disks.
   - Tape (tape out), select a clone pool that uses only tape devices.

10. Select **Continue on save set error** to force the NetWorker software to skip invalid save sets and to continue the clone operation.
If this option is not selected (default setting), an error message results and the clone operation stops if an invalid save set or invalid volume identifier is encountered.

11. To restrict the number of clone instances that can be created for any save set that is included in the particular scheduled clone operation:
   a. Type a value in the Limit number of save set clones attribute.
      A value of zero (0) means that an unlimited number of clones might be created for this scheduled clone operation. The NetWorker software allows one copy of a save set on any given volume since a clone is created for each volume in the pool. Only one clone is created for each run of a scheduled clone operation.
   b. 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, the NetWorker software 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.

12. Select Enable to allow the clone session to run at its scheduled time.

13. In the Start Time attribute, perform either of the following:
   - Click the up and down arrows to select the time to start the clone session.
   - or
   - Type the time directly into the attribute fields.

14. From the Schedule Period attribute:
   a. Select Weekly by day or Monthly by day depending on how you want to schedule the clone session.
   b. Select the days of the week or month on which the scheduled clone is to occur.

15. To repeat the clone session within a day, specify an Interval time in hours.
    For example, if the start time is 6 a.m., and the interval is 6 hours, then the clone session will run at 6 a.m., 12 p.m., and 6 p.m.

16. If the Limit the number of save set clones value is set, then the repeat clone session skips those save sets in the pool for which the specified number of clones already exists.

17. Click the Save Set Filters tab to specify the save sets to be included in this scheduled clone session.
   To limit save sets by various filter criteria, perform either of the following:
   - Select the clone save sets that match selections.
   - or
   - Select the clone specific save sets to explicitly identify the save sets to be cloned.

18. Click OK to save the scheduled clone session.
Displaying a list of the save sets that will be cloned based on the filter criteria

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.

Cloning save sets that match selection criteria

To clone save sets that match selection criteria, specify selection criteria to limit the save sets that will be included in this scheduled session. You can select the following criteria:

- Groups (savegroups)
- Clients (client resources)
- Pools (backup pools)
- 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)

Cloning specific save sets

Following this procedure to clone specific save sets.

Procedure

1. Type the specific save set ID/clone ID (SSID/clonid) identifiers in the **Clone specific save sets** list box.
2. Type each SSID/clonid value on a separate line.
3. You can query save set IDs/clone IDs by using one of the following methods:
   - Selecting the Administration > Media user interface
   - Using the mminfo command

Starting scheduled clone operations manually

You can start a scheduled clone session 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 a clone resource in the right pane.
4. Click Start.

Results

You can also start a scheduled clone from the NetWorker Monitoring feature.

Monitoring scheduled clone operations

In the Monitoring window of the Administration GUI, you can view the following:

- Status of scheduled clone sessions
- Scheduled clone's last start and end time
Completion status of each save set that is included in the scheduled clone

Viewing the clone status of a save set

To determine whether save set on a volume is a clone, or was cloned, check the window on the Query Save Set tab on a volume that has been cloned, or is a clone.

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.

Volume cloning uses \texttt{nsrclone}. However, it uses the volume name as an argument. Cloning in the NetWorker software operates at the save set level and does not specifically duplicate tape volume. This might result in multiple volumes being used.

The following describes the volume cloning process:

1. Instructs \texttt{nsrclone} to clone all of the save sets that exist on a particular volume.
2. When volumes are cloned, a list of all of the save sets that reside on them is created, and these in turn are then cloned.
3. Save sets that begin (header sections of continued save sets) on a specified volume will be completely copied:
   - Volumes may be requested during the cloning operation in addition to those specified on the command line.
   - Save sets that reside on the specified volumes that begin elsewhere (middle sections or tail sections of continued save sets) are not cloned.

Cloning a save set

Follow this procedure to clone a save set.

Procedure

1. From the Administration window, click Media.
2. In the expanded left pane, select Save Sets.
3. In the right pane:
   a. Click the Query Save Set tab.
   b. Use the Query Save Set tab to specify options to limit the range of save sets displayed.
   c. All query options are optional except for the date. A date range must be selected.

\textbf{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
5. Use the **Copies** attribute to limit the search to only those save sets that have already been cloned:
   a. Select a boolean value from the list:
      - Greater than (>)
      - Equal to (=)
      - Less than (<)
   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

   **Note**

   A long date range might 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 values that can be selected include the following:
   - All
   -Browsable
   -Recyclable
   -Scanned-in
   -Recoverable
   -Suspect

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. From the **Save Set** list, select the save sets to clone.
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.

### Scripted cloning

As of NetWorker 7.6 SP1, most of the functionality provided in the `nsrclone.exe` command is now provided in the NMC Clone resource user interface. However, for some situations or circumstances, the use of the `nsrclone.exe` command within a script can still have advantages. For example, a scripted cloning solution could be used for any of the following scenarios:

- To control the conditions before cloning occurs. For example, following a specific event or test, or as part of a workflow.
- To control the actions after cloning has been successful. For example, deleting files, or moving data as part of a workflow.
- To control the cloning as part of an enterprise management scheduler that is independent of NetWorker scheduling or NMC.
- To create multiple clones. For example, clone 1 on disk, clone 2 to tape, each with specific dependencies, timing, and logic.

**Note**

When using the scripted cloning feature, use the latest versions of NetWorker software. This will minimize the complexity of the logic in the cloning script.

### NetWorker 7.6 Service Pack 1 enhancements

As of NetWorker 7.6 SP1, most of the functionality provided in the `nsrclone` command is now provided in the NMC Clone resource user interface. The updated `nsrclone` command also contains a number of enhancements that can significantly reduce the size and complexity of any script. Table 3 on page 62 provides the descriptions of the options that can be used with the `nsrclone` command.

### NetWorker 7.5 enhancements

As of NetWorker 7.5, the `nsrclone` command has been enhanced to provide greater flexibility when selecting save sets for cloning by:

- Clients
- Groups
- Save set names
- Save set levels
- The number of valid copies
- The number of clones not yet created in the target pool
nsrclone option descriptions

The following table provides the descriptions of the options that can be used with the nsrclone command.

Table 3 Descriptions of nsrclone options

<table>
<thead>
<tr>
<th>Options</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>-C less than copies in target pool</td>
<td>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 be used only with the -t or -e option.</td>
</tr>
<tr>
<td>-l level or range</td>
<td>Specifies the level or n1-n2 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 set0 also means full, can be used. More than one level can be specified by using multiple -l options and the -l n1 to n2 range format. This option can be used only with the -t or -e option.</td>
</tr>
<tr>
<td>-N save set name</td>
<td>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 be used only with the -t or -e option.</td>
</tr>
<tr>
<td>-c client name</td>
<td>Specifies the save sets in the particular client. More than one client name can be specified by using multiple -c options. This option can be used only with the -t or -e option.</td>
</tr>
<tr>
<td>-g group name</td>
<td>Specifies the save sets in the particular group. More than one group name can be specified by using multiple -g options. This option can be used only with the -t or -e option.</td>
</tr>
</tbody>
</table>

Using the nsrclone options

The following examples show how various options can be used with the nsrclone command:

1. Copy all save sets created in the last twenty-four hours for the 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
   ```

2. 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
   ```
3. 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
```

Using the nsrclone command to specify a browse and retention policy

When using nsrclone you are able to specify a browse and retention policy from the command prompt.

Specifying a retention policy

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.

Specifying a browse policy

To specify a browse policy from the command prompt, use the nsrclone command with the -w option when creating a clone save set.

Note

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.

NSR clone resources

Clone resources that are created with the nsradmin program's NSR clone resources cannot be edited as scheduled clone resources in the NetWorker Administration graphical user interface GUI.

To avoid this issue, perform one of the following:

Procedure

- Create scheduled clone resources in the Administration interface. Scheduling clone operations on page 55 provides more information.
- Create a NSR clone resource, if required 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"
```

Cloning archived data

You can schedule a clone session to clone archive data or clone archive data manually.
Scheduling a clone session for archive data

Use the following procedure to set up a scheduled clone session for archive data.

Procedure
1. Follow the steps in Scheduling clone operations on page 55.
2. Select an archive pool as one of your save set filter criteria.

Cloning an archive volume manually

Use the following procedure to manually clone an archive volume.

Procedure
1. From the Administration window, click Media.
2. In the expanded left pane, select Save Sets.
3. In the right pane, click the Query Save Set tab.
4. In the Pool attribute:
   a. Select an archive pool from the list.
   b. Make other selections, as appropriate, to limit the save set search criteria.
      Starting scheduled clone operations manually on page 58 provides more information.
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.
10. Click Yes on the confirmation screen.

Considerations to improve cloning performance

Cloning can be performed in parallel so that multiple clone sessions can be active at the same time. However, the number and speed of this will depend on the devices that are being used and the method that is employed to start the cloning operation.

Consider the following:
- Automatic cloning is based on a savegroup and is a single-threaded process.
- For a given group, the NetWorker software runs only one clone at a time, regardless of the parallelism setting.
- Other groups that have auto-clone configured are able to run in parallel. However, they will also run only one clone at a time, assuming that there is no contention for volumes or devices.

Cloning validation

Clone data does not require validation because the data is read from the source in its native and self-describing form and then it is written to the target. The action of creating a
clone validates the ability to read the source data from the media. Therefore, subsequent
clone operations based on the clone will also be validated as further copies are created.
If there are actions that are expected after a clone operation, then it is likely that some
form of validation is used. This is important if the follow-on action has a destructive or
irreversible nature, such as the deletion of the source data through expiration or
relabeling.
For individual save sets, use the mminfo command to check that the clone save set is
valid and not in an aborted or error state.
Additional clone copies can also be used to:
• Validate that the save set is able to be read.
• Provide additional assurance and protection.
Although a check of individual save sets may help confirm a successful clone operation,
it does not confirm that recovery is possible:
• Additional save sets may also be required as part of the recovery.
• Always ensure that all save sets have been identified and cloned successfully.
• Application-based backups are a particular example where multiple save sets may be
required.

Displaying the backup versions in the GUI
After the scanning the data is complete, you can display the backup in the NetWorker
User program.
You can display the data by using one of the following methods:
Procedure
• If the application object is present in the most recent backup, you can view versions
for that application object. The versions are not cached, so a newly scanned version
should be detected if present:
  a. From the View Versions pane, look for the savetime that the data was scanned.
  b. If the savetime is found, choose this savetime as the new browse time to proceed.
  c. Use the Change Browse Time attribute to set the time slightly ahead of the most
recent save set that was scanned.
• If you are restoring from an incremental backup:
  a. Validate that the prior full and all incremental backups are also visible as backup
versions.
  b. Run View Versions for the application object.
• If the scanned backup version does not appear in the NetWorker User program,
validate the rollover save set.
CHAPTER 5
Recovering Data from Clones

This chapter contains the following topics:

- Clones recovery ................................................................. 68
- Recovery scenarios ............................................................ 68
- Required save sets and volumes for recovery of cloned data .... 71
- Recovery tasks ................................................................. 74
Clones recovery

When using cloning, ensure that you can recover the cloned save sets for all of the recovery scenarios that are expected to occur. These recovery scenarios and the steps to recover the cloned save sets are likely to be specific to the situation. Recovery scenarios on page 68 provides details.

To ensure that the recovery of cloned data:

- Verify that all relevant recovery scenarios have been accounted for as described in Recovery scenarios on page 68. For example, if you expect to rely on the clone copy for recovery, then you must ensure that the recovered save sets come from the clone copy and not from the original volume. This is important for situations where both or all copies are available, as well as when the original is not. Selecting clone volumes to recover data from on page 74 provides details.

- Ensure that all the required save sets and volumes are available for recovery. Required save sets and volumes for recovery of cloned data on page 71 provides detailed information.

- Ensure that recovery procedures are in place and have been regularly tested as described in Recovery tasks on page 74.

Recovery scenarios

When a recovery operation is initiated, there are two common assumptions about recovery operation.

- That the recovery will be performed within a short period of time after the backup (hours or days).

- That the recovery will use the original data volumes and that the backup server will be fully operational. You can use the standard NetWorker recovery procedure because the backups are present in both the client file indexes and the media database. Required save sets and volumes for recovery of cloned data on page 71 provides details.

However, if the recovery operation occurs after the NetWorker browse or retention periods have expired or following a site or building loss, then the volumes may not be readily available and additional actions might be required. Table 4 on page 69 details the recovery scenarios and necessary actions.

Browse and retention periods

In many restore operations, the request to restore the data arrives soon after the backup has completed. In these circumstances the browse and retention periods are likely to be still valid and recovery is simple. Required save sets and volumes for recovery of cloned data on page 71 provides details on how to restore cloned data in this scenario.

In cases where the browse and retention periods have expired, additional effort might be required to perform a restore operation. It is important to consider this when determining the browse and retention periods for the backup and the clone copies. Consider the browse and retention policies on page 31 provides more information on how to restore cloned data in this scenario.
Identifying the recovery options

If the recovery is not readily available, perform the following:

**Procedure**

1. Identify the backup or clone save sets that are required.
2. Investigate the cause and attempt to remedy the situation. Table 4 on page 69 provides details.
3. Seek alternative recovery options if required. Recovery tasks on page 74 provides details.

**Results**

The NetWorker software has various log files that contain information about the volumes, status, and history of cloning operations. These can be viewed and monitored from the NetWorker Administration window or recovered from previous server backups.

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.

Review the recovery scenarios

If the recovery is not immediately available or successful, review the following list of recovery scenarios to help determine the cause and the resolution if available.

**Table 4 NetWorker restore scenarios**

<table>
<thead>
<tr>
<th>Restore scenario</th>
<th>Description</th>
<th>Section</th>
</tr>
</thead>
<tbody>
<tr>
<td>Recovering original or clone data that is browsable. The save sets appear in both the client file index and in the media database.</td>
<td>The backups are present and browsable in both the client file indexes and in the media database.</td>
<td>Restoring cloned data that is browsable in the client file index on page 75</td>
</tr>
</tbody>
</table>
| The browse period has elapsed and the client file index entries have been purged. | The client index information has been purged because the browse period has elapsed. Although you can use the media database to identify the volumes and the save sets, you cannot perform a partial or item-level recovery operation. If the browse policy has elapsed, you can:  
  - Use the nsrck -L7 -t command to recover the client file index entries.  
  - Use the scanner command to recreate the client file index entries. | Restoring recyclable save sets to the client file index on page 78 |
| The browse and retention periods have both elapsed but the volume has not been recycled since the data that | The media database entries have been marked as expired but the volume has not been recycled (relabeled). If the volume has not been recycled, then the media database entries will still exist. You must | Restoring recyclable save sets to the client file index on page 78 |
### Table 4 NetWorker restore scenarios (continued)

<table>
<thead>
<tr>
<th>Restore scenario</th>
<th>Description</th>
<th>Section</th>
</tr>
</thead>
<tbody>
<tr>
<td>is still within the retention period.</td>
<td>mark the media database entries in the media database as eligible for recovery.</td>
<td></td>
</tr>
<tr>
<td>The browse and retention periods have both expired and the volume has been recycled.</td>
<td>If the volume has been recycled, then the media entries have been purged. In this case the data is longer available to recover from and alternative recovery sources will need to be used.</td>
<td>Selecting clone volumes to recover data from on page 74</td>
</tr>
<tr>
<td>One or more volumes are missing or are offline.</td>
<td>Some or all of the original backup volumes are no longer available for restore:</td>
<td>• The <em>EMC NetWorker Administration Guide</em> provides detailed information.</td>
</tr>
<tr>
<td></td>
<td>• If the volumes are offsite or in storage, then they can be easily recalled and made available to the online NetWorker server so that the recovery operation can continue. In this situation the media database entries are still available and valid. A mount operation or library inventory may also be required to make the volumes available.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• If the media database entries are <em>not</em> available or are invalid, use the scanner command to repopulate the media entries so that the NetWorker server knows what data is on that volume.</td>
<td>• Restoring save sets that are not in the media database on page 80</td>
</tr>
<tr>
<td>The clone volume does not contain all of the save sets that are required to be recovered.</td>
<td>If the clone volumes do <em>not</em> contain all of the necessary data for the recovery, then the number of available recovery options might be limited. Data might be able to be recovered, if:</td>
<td>• Restoring recoverable save sets to the client file index on page 76</td>
</tr>
<tr>
<td></td>
<td>• The original bootstrap (media and client index) information is available.</td>
<td>• Restoring save sets that are not in the media database on page 80</td>
</tr>
<tr>
<td></td>
<td>• The original volumes still exist and can be used for recovery.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>A recovery of that data might not be possible in cases where:</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• No bootstrap backups exist for the period of time where the recovery is requested.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• The original data volumes are missing or have been recycled.</td>
<td></td>
</tr>
<tr>
<td>The NetWorker server does not have knowledge or any database records of the backup.</td>
<td>The NetWorker server has been rebuilt or has been recently recovered and all or most records of the previous backups are missing. A full recovery of the media database and client file indexes is required before any client recovery operation can be initiated. The recovery should include media and client index entries for all the volumes, clients, and dates</td>
<td>The <em>EMC NetWorker Disaster Recovery Guide</em> provides detailed information.</td>
</tr>
</tbody>
</table>
Table 4 NetWorker restore scenarios  (continued)

<table>
<thead>
<tr>
<th>Restore scenario</th>
<th>Description</th>
<th>Section</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>available. This relies on the NetWorker server bootstrap backups.</td>
<td></td>
</tr>
</tbody>
</table>

**Required save sets and volumes for recovery of cloned data**

Before initiating a recovery it is important to ensure that all of the required save sets and volumes are available for recovery.

When clone volumes are being used, ensure that all the clone save sets are available for recovery. Selecting clone volumes to recover data from on page 74 provides details.

**Generating a media database listing of all of the save sets**

Use the following procedure to generate a media database listing of all of the save sets.

**Procedure**

1. At the command line prompt on the NetWorker server, type the following command to generate a list of the cloned save sets in the media database:

   ```
   mminfo -S -s NW_server_name -c NW_client_name
   -q "group=group_name,savetime>date1,savetime<date2"
   -ot 1>output.txt 2>&1
   ```

   where:
   - `NW_server_name` is the name of the NetWorker server host.
   - `NW_client_name` is the name of the NetWorker client host.
   - `group_name` is the name of the group which contained the NetWorker client when the backup occurred.
   - `date1` is at least one day before the date range of the NetWorker clone to be restored.
   - `date2` is at least one day after the date range of the NetWorker clone to be restored.

   For example, to list the save set details which reside on a NetWorker server called `krkr-pdc.krkr.local`, an NMM client `krkr8x64.krkr.local` named in a group called `grupa2` on dates Dec 14 13:48:00 2010 and Dec 15 13:57:00 2010, use the command:

   ```
   mminfo -S -s krkr-pdc.krkr.local -c krkr8x64.krkr.local -q "group=grupa2,savetime>12/14/2010 13:48:00,savetime<12/15/2010 13:57:00" > out3.txt
   ```

2. Edit the output.txt file, which resides in the same directory where the `mminfo` command was run.

   If the output file contains the following message, the media database does not contain the NetWorker save sets for the client or query options specified:

   ```
   mminfo: no matches found for the query
   ```
• Make adjustments to the query options specified in the mminfo command.
  or
• Restore the media database. Restoring save sets that are not in the media
database on page 80 provides details.

Determining the status of a save set in the media database
To determine the status of a save set in the media database, use the mminfo command. You can use the ssflags attribute to provide a summary of the status of each save set.

When generating a report of the ssflags summary of save sets:
• An r in the ssflags output denotes that a save set is recoverable and that it has exceeded its defined browse policy.
• An E in the ssflags output denotes a save set that is eligible for recycling and that it has exceeded its defined retention policy. This is also referred to as an expired save set.
  In the case of incremental or differential save sets, the ssflags value will contain an E only when all dependent incremental, differential, or full backups have also exceeded their defined retention policy period.
  When all save sets on a volume are eligible for recycling, the volume can be overwritten.

Save set requirements

Note
Do not use these procedures until you are familiar with all of the save set requirements.

Recovering data from media that has either expired or is recyclable requires that you identify the save sets for the backup:
• If you are know the list of required save sets that are to be recovered, perform the steps outlined in Using the backup time to list all of the save sets on page 72.
• If you do not know all of the required save sets that are to be recovered, perform the steps outlined in Using savetime to determine the full set of save sets to recover on page 73.

Using the backup time to list all of the save sets
If you are familiar with the required save set for the NetWorker software, you can use the backup time to ensure that all of the cover save sets are displayed:

```
mminfo -v -ot -q "group=group_name,saveset>date1,saveset<date2" -r "ssid, cloneid, nsavetime, ssflags, level, savetime(22), ssbrowse, ssretent, name, client, volume" 1>output.txt 2>&1
```

where:
• group_name is the name of the group which contained the NetWorker client when the backup occurred.
• date1 is at least one day before the date range of the NetWorker clone to be restored.
• date2 is at least one day after the date range of the NetWorker clone to be restored.
  This query will return all of the save sets for the group in the time range specified. The -ot flag sorts the return all of the save sets for the group in the time range specified. The -ot flag sorts the save sets by time and the information is stored in a file called output.txt. This file resides in the same directory from which the mminfo command was run.
### Note

If you experience restore issues using this easier method, use the procedures in Generating a media database listing of all of the save sets on page 71 to validate the output.

### Using savetime to determine the full set of save sets to recover

You can use the mminfo command to identify the required savetime range for the backup version that is being restored by querying the media database. The savetime range is used to query the media database.

The savetime range is the day before \((date_1)\) and the day after \((date_2)\) the date of the backup which is to be restored.

### Note

If the backup that is to be restored was an incremental level backup or a differential level backup, you must increase the savetime range to include the sequence of the full and the level backups.

### Procedure

1. For the version of the backup that is being restored, identify the required savetime range.

   If you are restoring a file system, you might need to:
   a. Expand the savetime range to include the sequence of full and incremental backups.
   b. Adjust the savetime range accordingly.

2. Identify the save set name that was used to backup the filesystem that is being restored.

3. Use the savetime range to generate the media database listing for the backup:

   ```
   mminfo -S -s server -c client -q
   "group=group, savetime>date1, savetime<date2"
   ```

   For example, use the following command to restore a backup that occurred on 4/28/2010:

   ```
   mminfo -S -s bv-nwsvr-1 -c bv-accounting-1 -q
   ```

   where:
   - `bv-accounting-1` is the NetWorker client.
   - `bv-nwsvr-1` is the NetWorker server.
   - `BV-accounting-1_Group` is the group.

4. Identify the most recent full backup for the file system save set in the mminfo report.

   For NetWorker Snapshot Management (NSM) or NetWorker Module for Microsoft (NMM) file system savesets, identify the full backup by identifying a rollover save set. Rollover save sets have the following characteristics:
   - The save set name of the file system.
   - The save set name does not have \(K\) in the sflags.
Selecting clone volumes to recover data from

Review the following procedure to ensure that the recovery comes from the clone copy and not the original in situations where both or all of the copies are available.

The volume, either a clone or original volume, that is selected for a recovery operation is determined as follows.

**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.

   The *EMC NetWorker Administration Guide* provides information about changing the status of a 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)

5. Use the `nsmrm` command to specify that a volume is offsite. For example:

   ```
   nsmrm -o offsite -V volume_id
   ```

   The volumes required for recovery appear in the Required Volumes window of the NetWorker User program. The *EMC NetWorker Administration Guide* provides information on viewing volumes that are required for data recovery.

   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. The *EMC NetWorker Administration Guide* provides information on restoring a save set entry in the online indexes.

**Recovery tasks**

This section discusses recovery from cloned save sets to help you identify what save sets are required, and ensure that these save sets are in a state that can be used for recovery.

To restore the data from full and incremental backups:

- For each backup, repeat the tasks listed in this section until all of the incremental backups that occurred after the full backups have been recorded.
- To restore multiple clients, repeat the recovery tasks for each client.
Restoring cloned data that is browsable in the client file index

Recover cloned data that is browsable by using the standard NetWorker recovery procedure since the backups are present in both the client file indexes and are in the media database.

No special operation is required to recover cloned data. The *EMC NetWorker Administration Guide* provides detailed information.

For each save set, if the backup has expired but its save sets are still listed as recyclable in the *mminfo* output, you must restore the online client file indexes.

**Procedure**

1. For each save set, reset the browse and retention time:

   ```
   nsrcm -e time1 -w time2 -S SSID/cloneid
   ```

   where
   - *time1* is the required retention time.
   - *time2* is the required browse time.
   - *SSID* is the save set value recorded for each save set from the output of the *mminfo* command.

   If the *cloneid* is not identified with the -S option, the following error message appears:

   ```
   Save set ssid cannot be marked as notrecyclable. Please specify the ssid/cloneid of the particular clone instance.
   ```

2. For each save set, use its associated SSID and cloneid that is recorded in the List Required Save sets section to reset the save set to expired/recoverable:

   ```
   nsrcm -o notrecyclable -S SSID/cloneid
   ```

3. Repopulate the client file index with the save set information:

   ```
   nsrck -L 7 -t date client 1>nsrck.txt 2>&1
   ```

   where:
   - *date* is a date after the completion of the latest save set that will be restored.
   - *client* is the name of the NetWorker client.

   **Note**

   Ensure that the volume containing the index backup is available for mounting.

4. Review the output in nsrck.txt for errors once the command has completed:

   - If the following messages are reported, type the following command:

     ```
     nsrck -L 2 client
     ```

     where *client* is the name of the NetWorker client.

     **Messages:**

     19779:nsrck: Please run `nsrck clientname`
     9348:nsrck: The index recovery for 'clientname' failed.
     39078:nsrck: SYSTEM error: The operation completed successfully.
File attribute messages such as the following will not impact the restore and can be safely ignored:

```
32222:uasm: Warning: Some file attributes were not recovered: C:\Program Files\Legato\nsr\index\clientname\db6\tmprecov\C\Program Files\Legato\nsr\index\clientname\db6\`
```

If the nsrck command fails with the error "xxxxx", the index backup might no longer be referenced in the media database.

Use the following command to scan all SSIDs recorded for each save set:

```
scanner -i -S SSID device
```

where:
- **SSID** is the save set id of the save set that will be restored.
- **device** is the device containing the volume for the save set to be restored.

5. Ensure that the NetWorker User program is closed on the NMM clients before running the scanner command. If the program is open while scanner is run, the scanner command may fail with the following errors:

- For NetWorker 7.6.1 and earlier:
  
  "Index error, flush Failed"

- For NetWorker 7.6.2 and later:

  "8829:scanner: (ssid 2772567781) index error, store failed"
  "39077:scanner: error, Cannot unlink the existing key file C:\Program"
  "Files\Legato\nsr\index\bv-e2007sp3-ccr\db6\4d420000\4d4206e1.k0 before re-creating it. Error "Permission denied"

6. For each save set, modify the browse times of the existing save sets, if browse and retention times set by scanner are not a long enough duration to complete recovery procedures:

```
snrmm -s NetWorker_server_name -w time2 -S SSID
```

where:
- **NetWorker_server_name** is the name of the NetWorker server.
- **time2** is the new browse time.
- **SSID** is the save set value recorded for each save set.

7. Ensure that the new browse dates for the save sets are far enough in the future to allow sufficient time for the restore to complete.

8. Restore the data. The *EMC NetWorker Administration Guide* provides detailed information.

---

**Restoring recoverable save sets to the client file index**

If the backup save sets for the rollover, display, metadata and cover save set that are recoverable, they can be made browsable for the required length of time to perform the restore operation. For example sflags=vrf.
Procedure

1. For each display, metadata and rollover save set, modify the browse and retention times of the existing save sets:

   \texttt{nsrmm -s NetWorker\_server\_name -e time1 -S SSID}

   where:
   - \texttt{NetWorker\_server\_name} is the name of the NetWorker server.
   - \texttt{time1} is the new retention time.
   - \texttt{SSID} is the save set value recorded for save set.

   \textbf{Note}

   Ensure that the new browse and retention dates for the save sets are far enough in the future to allow sufficient time for the restore operation to complete.

2. Repopulate the client file index on the NetWorker server with the save set information:

   \texttt{nsrck -L 7 -t date client 1>nsrck\_txt 2>&1}

   where:
   - \texttt{date} is a date after the completion of the latest save set that will be restored.
   - \texttt{client} is the name of the NetWorker client.

   \textbf{Note}

   Ensure that the volume containing the index backup is available for mounting.

3. Review the output in \texttt{nsrck\_txt} for errors once the command has completed.

   Consider the following:
   - If the following messages are reported, run the following command:

     \texttt{nsrck -L 2 client}

     where \texttt{client} is the name of the NetWorker client.

     Messages:

     - 19779:nsrck: Please run `\`nsrck clientname``
     - 9348:nsrck: The index recovery for ' clientname ' failed.
     - 39078:nsrck: SYSTEM error: The operation completed successfully.

   - File attribute messages such as the following will not impact the NetWorker restore and can be safely ignored:

     - 32222:uasm: Warning: Some file attributes were not recovered: C:\Program Files\Legato\nsr\index\clientname\db6\tmprecov\C
       \texttt{\Program Files\Legato\nsr\index\clientname\db6\}

   - If the \texttt{nsrck} command fails with the error "xxxxx", the index backup might no longer be referenced in the media database. Use the following command to scan all SSIDs recorded for each save set:

     \texttt{scanner -i -S SSID device}

     where:
SSID is the save set id of the save set that will be restored.

device is the device containing the volume for the save set to be restored.

4. Ensure that the NetWorker User program is closed on the NMM clients before running the scanner command. If the program is open while scanner is run, the scanner command may fail with the following errors:

- For NetWorker 7.6.1 and earlier:
  "Index error, flush Failed"

- For NetWorker 7.6.2 and later:
  "8829:scanner: (ssid 2772567781) index error, store failed"
  "39077:scanner: error, Cannot unlink the existing key file C:\Program"
  "Files\Legato\nsr\index\bv-e2007sp3-ccr\db6\4d420000\4d4206e1.k0 before re-creating it. Error "Permission denied"

5. For each save set, modify the browse times of the existing save sets. If browse and retention times set by scanner are not a long enough duration to complete recovery procedures:

```
nsrmm -s NetWorker_server_name -w time2 -S SSID
```

where:

- `NetWorker_server_name` is the name of the NetWorker server.
- `time2` is the new desired browse time.
- `SSID` is the save set value recorded for each save set.

**Note**

Ensure that the new browse dates for the save sets are far enough in the future to allow sufficient time for the restore to complete.

6. Restore the data. The *EMC NetWorker Administration Guide* provides detailed information.

**Restoring recyclable save sets to the client file index**

For each save set, if the backup has expired but its save sets are still listed as recyclable in the mminfo output, you must restore the online client file indexes.

**Procedure**

1. For each save set, reset the browse and retention time:

```
nsrmm -e time1 -w time2 -S SSID/cloneid
```

where:

- `time1` is the required retention time.
- `time2` is the required browse time.
- `SSID` is the save set value recorded for each save set from the output of the mminfo command.
If the cloneid is not identified with the -S option, the following error message appears:

```
Save set ssid cannot be marked as notrecyclable. Please specify the ssid/cloneid of the particular clone instance.
```

2. For each save set, use its associated SSID and cloneid that is recorded in the List Required Save sets section to reset the save set to expired/recoverable:

```
nsrcm -o notrecyclable -S SSID/cloneid
```

3. Repopulate the client file index with the save set information:

```
nsrck -L 7 -t date client 1>nsrck.txt 2>&1
```

where:

- **date** is a date after the completion of the latest save set that will be restored.
- **client** is the name of the NetWorker client.

**Note**

Ensure that the volume containing the index backup is available for mounting.

4. Review the output in nsrck.txt for errors once the command has completed:

- If the following messages are reported, type the following command:

```
nsrck -L 2 client
```

where **client** is the name of the NetWorker client.

**Messages:**

19779:nsrck: Please run `nsrck clientname`
9348:nsrck: The index recovery for ' clientname ' failed.
39078:nsrck: SYSTEM error: The operation completed successfully.

- File attribute messages such as the following will not impact the NetWorker restore and can be safely ignored:

```
32222:uasm: Warning: Some file attributes were not recovered: C:\Program Files\Legato\nsr\index\clientname\db6\tmprecov\C
```

- If the nsrck command fails with the error "xxxxx", the index backup might no longer be referenced in the media database. Use the following command to scan all SSIDs recorded for the save sets:

```
scanner -i -S SSID device
```

where:

- **SSID** is the save set id of the save set that will be restored.
- **device** is the device containing the volume for the save set to be restored.

5. Ensure that the NetWorker User program is closed on the NMM clients before running the scanner command. If the program is open while scanner is run, the scanner command may fail with the following errors:

- For NetWorker 7.6.1 and earlier:

```
"Index error, flush Failed"
```
Recovering Data from Clones

- For NetWorker 7.6.2 and later:

  "8829:scanner: (ssid 2772567781) index error, store failed"
  "39077:scanner: error, Cannot unlink the existing key file C:\Program"
  "Files\Legato\nsr\index\bv-e2007sp3-ccr
  \db6\4d4d0000\4d4d6e1.k0 before re-creating it. Error
  'Permission denied"

6. Modify the browse times of the existing save sets, if browse and retention times set by scanner are not a long enough duration to complete recovery procedures:

   `nsrmm -s NetWorker_server_name -w time2 -S SSID`

   where:
   - **NetWorker_server_name** is the name of the NetWorker server.
   - **time2** is the new browse time.
   - **SSID** is the save set value recorded for each save set.

   **Note**

   Ensure that the new browse dates for the save sets are far enough in the future to allow sufficient time for the restore to complete.

7. Restore the data. The *EMC NetWorker Administration Guide* provides detailed information.

**Restoring save sets that are not in the media database**

If the clones are no longer in the media database, you must scan the clone volumes to regenerate the media database and the client file index database for these save sets.

The following procedures are used to perform this task:

**Identifying the clone volumes that are required for scanning**

The scanning procedure is used to rebuild index and media database entries.

- When restoring from a full backup, the volumes from the date of the full backup are required to recover the data from.
- When restoring from an incremental backup, the volumes from the day of the incremental backup to the most recent full backup are required to recover the data from.

*Selecting clone volumes to recover data from on page 74* provides information on how to ensure that the recovery comes from the clone copy and not the original in situations where both or all of the copies that are available.

**Note**

If other volumes are required to be scanned, review *Selecting clone volumes to recover data from on page 74* to identify what save sets are missing so that the additional volumes can be retrieved.

**Disabling the Idle Device Timeout attribute**

To prevent devices from being unloaded from the drives while scanner is in use, you must temporarily disable the Idle Device Timeout attribute, if it was configured.
Procedure
1. Connect to the NetWorker server through NMC.
2. Click Devices.
3. Right-click the device that is to be used.
4. Select Properties.
5. Click the Advanced tab.
6. Set the Idle Device Timeout value to 0.
7. Click OK.

Recovering the clone save sets that do not exist in the media database
If the NetWorker clone save sets that are required for a restore operation are no longer in
the media database, you must scan the clone volumes to regenerate the media and index
database for these save sets. You can use the scanner command to scan the volumes.

Procedure
1. Mount the volume containing the clone save sets into the drive.

Note
If the volume itself is no longer in the NetWorker media database, choose the option
load without mount while loading the tape.

2. From a command prompt on the NetWorker server, obtain a listing of the save sets on
the clone volume to generate a report of the save sets on the volume. Use the
following command:

```bash
scanner -v device 1>scanner_output.txt 2>&1
```

where device is the name of the device containing the volume.
For example:

```bash
scanner -v C:\device\clone 1>C:\output\5\scanner_output.txt 2>&1
```
or

```bash
scanner -v \\.\Tape0 1>scanner_output.txt 2>&1
```
3. Ensure that the NetWorker User program is closed on the NMM clients before
running the scanner command. If the program is open while scanner is run, the
scanner command may fail with the following errors:

- For NetWorker 7.6.1 and earlier:
  "Index error, flush Failed"

- For NetWorker 7.6.2 and later:
  "8829:scanner: (ssid 2772567781) index error, store failed"
  "39077:scanner: error, Cannot unlink the existing key file C:\Program"
  "Files\Legato\nsr\index\bv-e2007sp3-ccr\db6\4d420000\4d4206e1.k0 before re-creating it. Error
  'Permission denied"

4. Open the scanner_output.txt file, which resides in the same directory the
scanner command was run from.
5. If the `scanner_output.txt` file displays only the following message:

```
scanner: SYSTEM error: Cannot stat <device_name>: No such file or directory
```

   a. Check the device name specified in the `scanner` command for errors.
   b. Retry the `scanner` command with the correct device name.

Determining SSID of the required save sets

Use the following procedure to determine the SSID of the required save sets.

**Procedure**

1. Inspect the `scanner_output.txt` file to determine the SSIDs of the required save sets. These can be identified by using the following attribute values for each save set in the output file:
   - Client name
   - Save time
   - Level
   - Save set name

2. To perform the restore, including all dependent full and incremental save sets, determine the following information for all of the save sets:
   - SSID
   - Savetime
   - Save set name

**Note**

The SSID values will be used later in the procedure to scan the save sets back into the media database and the savetime will be used to validate that the repopulation of the client file index was successful.

**NOTICE**

If the date of the point-in-time restore was an incremental or differential backup level as denoted by the value in the level column, all save sets from the point-in-time restore to the last full level restore must be identified. In some cases, the associated full backup might be on a different volume.

Scanning the required save sets into the media database and the client file index

Depending on your IT procedures and urgency of the restore request, you might choose to scan individual save sets from the clone volumes. Scanning should be run to regenerate both the media database and client file index entries.

Consider:

- It is not possible to specify the scanning order when save sets are supplied through the `-S` parameter to `scanner`.
- The end-to-end process of recovering from scanned clones might take several days, so resetting the browse and retention times to a sufficient point-in-time in the future will help to ensure that the scanned save sets do not prematurely expire before you are finished restoring the data.
Procedure

1. Use the following command to scan the save sets:

   scanner -i -S SSID device 1>scanneri.txt 2>&1

   where:
   - **SSID** is the SSID recorded for save set.
   - **device** is the device with media that contains the save set.

2. Ensure that the NetWorker User program is closed on the NMM clients before running the **scanner** command. If the program is open while scanner is run, the **scanner** command may fail with the following errors:
   - For NetWorker 7.6.1 and earlier:
     "Index error, flush Failed"
   - For NetWorker 7.6.2 and later:
     "8829:scanner: (ssid 2772567781) index error, store failed"
     "39077:scanner: error, Cannot unlink the existing key file C:\Program" 
     "Files\Legato\nsr\index\bv-e2007sp3-ccr" 
     "db6\4d420000\4d4206e1.k0 before re-creating it. Error " 
     "Permission denied"

   **Note**
   It is critical that the cover save sets be scanned first.

3. Review the output of the **scanneri.txt** file for errors.

Validating that the save sets are in the client file index

For each save set that was scanned, you can use the **nsrinfo** command to validate that the data has been repopulated in the client file index.

**Procedure**

1. During the inspection of the scanner output, review the savetime recorded for the save sets.

2. Run the **nsrinfo** command against each savetime to confirm that the client file index was populated with the necessary save set details:

   nsrinfo -t exact_savetime client

   where:
   - **exact_savetime** is the savetime recorded from the scanner output.
   - **client** is the name of the NetWorker client.

   For example:

   nsrinfo -t 1292314893 krkr8x64
   scanning client 'krkr8x64' for savetime 1292314893(14.12.2010 09:21:33) from the backup namespace
   C:\LG_PLACEHOLDER_1492021383
   1 objects found
3. For all recorded savetimes, run the nsrinfo command against each savetime to confirm that the client file index was populated with the necessary save set details:

```
nsrinfo -t exact_savetime client
```

where:

- `exact_savetime` is the savetime recorded from the scanner output.
- `client` is the name of the NetWorker client.

Generating a media database listing of all of the save sets

Use the following procedure to generate a media database listing of all of the save sets.

**Procedure**

1. At the command line prompt on the NetWorker server, type the following command to generate a list of the cloned save sets in the media database:

```
mminfo -S -s NW_server_name -c NW_client_name
-q "group=group_name, savetime>date1, savetime<date2"
-ot 1>output.txt 2>&1
```

where:

- `NW_server_name` is the name of the NetWorker server host.
- `NW_client_name` is the name of the NetWorker client host.
- `group_name` is the name of the group which contained the NetWorker client when the backup occurred.
- `date1` is at least one day before the date range of the NetWorker clone to be restored.
- `date2` is at least one day after the date range of the NetWorker clone to be restored.

For example, to list the save set details which reside on a NetWorker server called `krkr-pdc.krkr.local`, an NMM client `krkr8x64.krkr.local` named in a group called `grupa2` on dates Dec 14 13:48:00 2010 and Dec 15 13:57:00 2010, use the command:

```
mminfo -S -s krkr-pdc.krkr.local -c krkr8x64.krkr.local -q "group=grupa2, savetime>12/14/2010 13:48:00, savetime<12/15/2010 13:57:00" > out3.txt
```

2. Edit the output.txt file, which resides in the same directory where the `mminfo` command was run.

If the output file contains the following message, the media database does not contain the NetWorker save sets for the client or query options specified:

```
mminfo: no matches found for the query
```

- Make adjustments to the query options specified in the `mminfo` command.

  or

- Restore the media database. Restoring save sets that are not in the media database on page 80 provides details.
Restoring the data

Restore the data. The *EMC NetWorker Administration Guide* provides detailed information.
Recovering Data from Clones
CHAPTER 6

Staging

This chapter contains the following topics:

- Staging overview ................................................................. 88
- The destination ..................................................................... 88
- Working with staging policies ............................................ 89
- Staging from the NetWorker Management Console .......... 92
- Staging from the command line ......................................... 92
Staging overview

NetWorker staging is a separate process but relies on the cloning mechanism. 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.

Staging example

In the following figure, the staging action will result in the deletion of the original save sets on the Volume A1, once they had been successfully staged (cloned) to volume B1. The Xs indicate that once a successful clone copy has completed, the original save sets are deleted. This is the difference between a clone and a stage operation. The save sets appear to move from one storage to another. The resulting save set is identical to that of the first, but in a different location.

The destination

A save set can be staged from one disk to another as many times as required. For example, a save set could staged from disk 1, to disk 2, to disk 3, and finally to a remote disk.
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 stage 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 after staging only a single set of save sets exists in either the source volumes or clone volumes.

**Working with staging policies**

This section describes how to work with staging policies.

The *EMC NetWorker Administration Guide* provides information on file type device (FTD) and advanced file type device (AFTD) 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 AFTD 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 AFTD.

**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.

**Note**

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.

**Note**

The adv_file device and its corresponding _AF_readonly device will both be selected automatically, even if only one device was selected as the source of 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.

**Note**

The Default volume can only be staged to the Default or Default Clone pool. Similarly, the Default Clone volume can only be staged to the Default or Default Clone pool and Archive data can only be staged to the Archive Clone pool. The other volume types can be staged to any pool. If the Clone pool that you have selected is restricted to storage node devices, you will also need to modify Clone Storage Node attribute.

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 filesystem partition that the file device is on. Staging continues until the low-water mark is reached.

**Note**

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 filesystem 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.

**Note**

The Max Storage Period attribute is used in conjunction with the filesystem Check Interval attribute. Once the Max Storage Period value is reached, staging does not begin until the next filesystem 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 filesystem checks.

**Note**

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. Click 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 filesystem 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.

**Note**
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.

**Editing a staging policy**

Use the following procedure to edit 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.

**Note**
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 the Name attribute.
5. Type the name for the new Staging resource in the Name attribute, edit any other attributes as appropriate.
6. Click OK.

**Deleting a staging policy**

Use the following procedure to delete a staging policy.

**Note**
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.

### Staging from the NetWorker Management Console

Staging a save set from the command prompt works differently than staging a save set from the NetWorker Management Console (NetWorker Console).

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 from the NetWorker Console, select save sets that belong to a single device.

### Staging from the command line

When staging from the command prompt, specify the save set IDs to be staged.

The NetWorker software stages all the save sets with the specified save set ID and then removes those save sets. That means 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:

```bash
nsrstage -m -S ssid/cloneid
```

### Finding the clone ID of a save set

To find the clone ID of a save set, use the `mminfo` command. For example:

```bash
mminfo -avot -r "volume,ssid,cloneid,name"
```

The *EMC NetWorker Command Reference Guide* or the UNIX man pages provide information about `nsrstage` or `mminfo` commands.
CHAPTER 7

NetWorker Module for Databases and Applications

This chapter contains the following topics:

**NOTICE**

NMDA does *not* support save set bundling for regular manual backups or NetWorker Snapshot Management (NSM) backups. NMDA performs save set bundling for regular scheduled Oracle backups *only*.

- NMDA save set bundling ................................................................. 94
- NMDA policy uniformity ................................................................. 96
NMDA save set bundling

If the NetWorker Module for Databases and Applications (NMDA) save set bundling is configured, NMDA automatically creates a save set bundle to group all dependent save sets from the same backup cycle. Save sets are dependent when two or more save sets are required to restore a database object.

A backup cycle includes the following:

- A level 0 incremental backup of the database object.
- All subsequent level 1 incremental backups that are dependent on the level 0 backup.

The *EMC NetWorker Module for Databases and Applications Administration Guide* provides details on NMDA support of full and incremental Oracle backups.

**Note**

NMDA does not support save set bundling for regular manual backups or NetWorker Snapshot Management (NSM) backups. NMDA performs save set bundling for regular scheduled Oracle backups only. Save set bundling automatically enables the following for Oracle:

- Improved staging. Oracle-aware staging causes NMDA Oracle save sets that have a dependency on each other to be staged together:
  - During automatic staging, if the staging criteria determine that a particular NMDA save set should be staged and the save set is part of a save set bundle, the NetWorker server stages the entire save set bundle.
  - During manual staging with the `nsrstage` command, if one or more save sets being staged are from a save set bundle, all the save sets in the bundle are staged.
- Policy uniformity. Policy uniformity is enabled automatically whenever you enable save set bundling. If you do not want to use save set bundling, you can still enable policy uniformity separately. *NMDA policy uniformity on page 96* provides more details.

**Note**

After a staging operation during which all the save sets in a bundle are staged, the resulting available space on the staging device might exceed the lower-water mark specified in the staging policy.

The *EMC NetWorker Administration Guide* provides details on how to work with staging policies and perform automatic and manual staging operations through the NetWorker server.

The *EMC NetWorker Module for Databases and Applications Administration Guide* provides information on how to configure save set bundling for NMDA scheduled backups.

If an error occurs during save set bundling, the bundling operation fails but the scheduled backup can finish successfully. Information about the bundling failure is printed to the savegrp output and to the NMDA debug file.
NetWorker staging restrictions

When planning the strategy for NMDA save set bundling, consider the following NetWorker staging restrictions.

- The NetWorker server cannot simultaneously stage all the save sets from a save set bundle if some of the save sets were backed up to separate volumes. The server simultaneously stages save sets only if they are located on the same staging volume. Splitting a save set bundle across volumes on page 96 provides more information. To ensure the proper staging of all the save sets from a save set bundle, do not split the backup between different staging volumes. If required, split the backup into different backup cycles, with each cycle going to a separate volume.

- NetWorker staging policies must not cause the save sets of an NMDA backup cycle to be staged before the cycle is complete. For example, if a 1-week NMDA cycle starts on Sunday, the staging policy must not cause the partially complete save set bundle to be staged before the final backup of the cycle occurs on Saturday. To prevent a staging operation from splitting an NMDA backup cycle, adjust the NetWorker staging policy accordingly. For example, adjust the policy so that older save sets are staged before new ones, or adjust the high-water and low-water marks.

The *EMC NetWorker Administration Guide* provides details on how to work with staging policies and perform automatic and manual staging operations through the NetWorker server.

Save set bundling with NMDA

The NMDA program nsrdasv automatically places save sets into a save set bundle at the end of a scheduled backup.

To perform save set bundling:

- Operate NetWorker privileges are required.
- The nsrdasv program connects to the Oracle database by attempting to use the login and password from the RMAN script.
- If a login and password are not available from the script, the program uses the ORACLE_SID value from the NMDA configuration file to search the nwora.res file for the NSR_ORACLE_CONNECT_FILE parameter, and uses the connection strings from the specified connection file.
- After connecting to the Oracle database, the nsrdasv program obtains all the required information about the backups by using the V$ views. The *EMC NetWorker Module for Databases and Applications Administration Guide* provides more details on the nwora.res file and the requirements of save set bundling.
- The nsrdasv program creates a save set bundle for each incremental level 0 backup.
- The program adds the save sets from subsequent incremental backups to the bundles of the level 0 backups they are dependent on. Save set bundling for a 1-week scheduled backup cycle of a tablespace on page 96 and Save set bundle join on page 96 illustrate different scenarios for how the save set bundle is formed.
- The name that the nsrdasv program assigns to a save set bundle is the save time of the oldest save set in the bundle.
- After a scheduled backup, the NetWorker server stores the save set bundle name and the list of save sets it contains in the media database. You can view the bundle information by using the mminfo command, as described in Save set bundling information in the media database on page 96.
Save set bundling for a 1-week scheduled backup cycle of a tablespace

A 1-week scheduled backup cycle of a tablespace includes a level 0 backup of the tablespace on Sunday and a level 1 backup every other day of the week. The save set bundle for the cycle is created during the Sunday backup. Save sets from each level 1 backup are added into the same bundle. The complete bundle contains the save sets from the seven daily backups of the tablespace. A new bundle is created for the next backup cycle during the following week.

Save set bundle join

This example illustrates a scenario where NMDA combines existing bundles into a new save set bundle.

Two save set bundles are created by separate level 0 backups of files A and B. Then a new backup set is created by a level 1 backup of both files A and B. As the new backup set is dependent on both of the preceding level 0 backups, NMDA combines all three backups into the same save set bundle.

Splitting a save set bundle across volumes

In this example, a save set bundle is split across multiple volumes. A level 0 backup of file A is performed to volume A. An incremental backup of file A is then performed to volume B. Although both backups are recorded as belonging to the same save set bundle, the save set bundle is split across volumes. During staging, only the save sets on the same volume can be staged together.

Save set bundling information in the media database

The NMDA software stores information about each save set bundle in the NetWorker media database. Query the media database by using the NetWorker command, mminfo, with the appropriate options:

- The mminfo -r command can display the name of the bundle associated with a save set. For example, the following command displays a list of all save sets and their bundles:

  mminfo -a -r "ssid,ssbundle"

- The mminfo -q command can display all the save sets in a specific bundle. For example, the following command displays all the save sets in the bundle named 12983479182:
mminfo -a -q "ssbundle=12983479182"

The EMC NetWorker Command Reference Guide and the UNIX man pages provide more information on the mminfo command and its available options.

NMDA policy uniformity

If policy uniformity is enabled, NMDA automatically enforces the uniformity of the browse and retention policies between all the dependent save sets in a scheduled Oracle backup cycle (whether or not save set bundling is enabled).

After NMDA performs an incremental Oracle scheduled backup, if the browse and retention policies of the save sets in the backup are longest than the policies of preceding dependent save sets in the same backup cycle, NMDA changes the policies of all save sets in the cycle to match the longest policy of the new incremental save sets. NMDA modifies the policies recorded in the NetWorker media database. As a result,
backups cannot expire and become recyclable before other dependent backups from the same backup cycle.

**Note**

NMDA does not support policy uniformity for regular manual backups and NetWorker Snapshot Management (NSM) backups. NMDA supports policy uniformity for regular scheduled backups only.

Policy uniformity does not depend on whether save sets are stored on separate volumes. For example, if parts of a save set bundle are split onto separate volumes, all the save sets in the bundle still receive the same browse and retention policies.

The *EMC NetWorker Module for Databases and Applications Administration Guide* provides information on how to configure policy uniformity for NMDA backups.