Dell EMC NetWorker

Version 19.2

Data Domain Boost Integration Guide

REV 01

November 2019

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

THE INFORMATION IN THIS PUBLICATION IS PROVIDED “AS-IS.” DELL MAKES NO REPRESENTATIONS OR WARRANTIES OF ANY KIND WITH RESPECT TO THE INFORMATION IN THIS PUBLICATION, AND SPECIFICALLY DISCLAIMS IMPLIED WARRANTIES OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE. USE, COPYING, AND DISTRIBUTION OF ANY DELL SOFTWARE DESCRIBED IN THIS PUBLICATION REQUIRES AN APPLICABLE SOFTWARE LICENSE.

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

CONTENTS

FIGURES

TABLES

Preface

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

If a product does not function correctly or does not function as described in this document, contact a technical support professional.

ⓘ Note: This document was accurate at publication time. To ensure that you are using the latest version of this document, go to the Support website https://www.dell.com/support.

Purpose

This document provides planning, practices, and configuration information for the use of DD Boost devices within a NetWorker backup and storage management environment.

Audience

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

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

Revision history

The following table presents the revision history of this document.

Table 1 Revision history

Revision	Date	Description
01	November 15, 2019	First release of the document for NetWorker 19.2.

Related documentation

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

- *NetWorker E-LAB Navigator*
  Provides compatibility information, including specific software and hardware configurations that NetWorker supports. To access E-LAB Navigator, go to https://elabnavigator.emc.com/eln/elnhome.
- *NetWorker Administration Guide*
  Describes how to configure and maintain the NetWorker software.
- *NetWorker Network Data Management Protocol (NDMP) User Guide*
  Describes how to use the NetWorker software to provide data protection for NDMP filers.
- *NetWorker Cluster Integration Guide*
  Contains information related to configuring NetWorker software on cluster servers and clients.
- *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.

- *NetWorker Updating from a Previous Release Guide*
  Describes how to update the NetWorker software from a previously installed release.
- *NetWorker Release Notes*
  Contains information on new features and changes, fixed problems, known limitations, environment and system requirements for the latest NetWorker software release.
- *NetWorker Command Reference Guide*
  Provides reference information for NetWorker commands and options.
- *NetWorker Data Domain Boost Integration Guide*
  Provides planning and configuration information on the use of Data Domain devices for data deduplication backup and storage in a NetWorker environment.
- *NetWorker Performance Optimization Planning Guide*
  Contains basic performance tuning information for NetWorker.
- *NetWorker Server Disaster Recovery and Availability Best Practices Guide*
  Describes how to design, plan for, and perform a step-by-step NetWorker disaster recovery.
- *NetWorker Snapshot Management Integration Guide*
  Describes the ability to catalog and manage snapshot copies of production data that are created by using mirror technologies on storage arrays.
- *NetWorkerSnapshot Management for NAS Devices Integration Guide*
  Describes how to catalog and manage snapshot copies of production data that are created by using replication technologies on NAS devices.
- *NetWorker Security Configuration Guide*
  Provides an overview of security configuration settings available in NetWorker, secure deployment, and physical security controls needed to ensure the secure operation of the product.
- *NetWorker VMware Integration Guide*
  Provides planning and configuration information on the use of VMware in a NetWorker environment.
- *NetWorker Error Message Guide*
  Provides information on common NetWorker error messages.
- *NetWorker Licensing Guide*
  Provides information about licensing NetWorker products and features.
- *NetWorker REST API Getting Started Guide*
  Describes how to configure and use the NetWorker REST API to create programmatic interfaces to the NetWorker server.
- *NetWorker REST API Reference Guide*
  Provides the NetWorker REST API specification used to create programmatic interfaces to the NetWorker server.
- *NetWorker 19.2 with CloudBoost 19.2 Integration Guide*
  Describes the integration of NetWorker with CloudBoost.
- *NetWorker 19.2 with CloudBoost 19.2Security Configuration Guide*
  Provides an overview of security configuration settings available in NetWorker and Cloud Boost, secure deployment, and physical security controls needed to ensure the secure operation of the product.
- NetWorker Management Console Online Help
  Describes the day-to-day administration tasks performed in the NetWorker Management Console and the NetWorker Administration window. To view the online help, click **Help** in the main menu.

- NetWorker User Online Help
  Describes how to use the NetWorker User program, which is the Windows client interface, to connect to a NetWorker server to back up, recover, archive, and retrieve files over a network.

Note: References to Data Domain systems in this documentation, in the UI, and elsewhere in the product include PowerProtect DD systems and older Data Domain systems.

- *Data Domain Boost Compatibility Guide*
  Provides compatibility information for DellEMC and third party applications, and Fibre Channel hardware solutions, that interoperate with Data Domain Boost (DD Boost) technology.

Special notice conventions that are used in this document

The following conventions are used for special notices:

NOTICE Identifies content that warns of potential business or data loss.

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

Typographical conventions

The following type style conventions are used in this document:

Table 2 Style conventions

Bold	Used for interface elements that a user specifically selects or clicks, for example, names of buttons, fields, tab names, and menu paths. Also used for the name of a dialog box, page, pane, screen area with title, table label, and window.
Italic	Used for full titles of publications that are referenced in text.
`Monospace`	Used for: • System code • System output, such as an error message or script • Pathnames, file names, file name extensions, prompts, and syntax • Commands and options
Monospace italic	Used for variables.
`Monospace bold`	Used for user input.
[ ]	Square brackets enclose optional values.
|	Vertical line indicates alternate selections. The vertical line means or for the alternate selections.
{ }	Braces enclose content that the user must specify, such as x, y, or z.
...	Ellipses indicate non-essential information that is omitted from the example.

You can use the following resources to find more information about this product, obtain support, and provide feedback.

Where to find product documentation

- https://www.dell.com/support
- https://community.emc.com

Where to get support

The Support website https://www.dell.com/support provides access to product licensing, documentation, advisories, downloads, and how-to and troubleshooting information. The information can enable you to resolve a product issue before you contact Support.

To access a product-specific page:

1. Go to https://www.dell.com/support.
2. In the search box, type a product name, and then from the list that appears, select the product.

Knowledgebase

The Knowledgebase contains applicable solutions that you can search for either by solution number (for example, KB000xxxxxx) or by keyword.

To search the Knowledgebase:

1. Go to https://www.dell.com/support.
2. On the **Support** tab, click **Knowledge Base**.
3. In the search box, type either the solution number or keywords. Optionally, you can limit the search to specific products by typing a product name in the search box, and then selecting the product from the list that appears.

Live chat

To participate in a live interactive chat with a support agent:

1. Go to https://www.dell.com/support.
2. On the **Support** tab, click **Contact Support**.
3. On the **Contact Information** page, click the relevant support, and then proceed.

Service requests

To obtain in-depth help from Licensing, submit a service request. To submit a service request:

1. Go to https://www.dell.com/support.
2. On the **Support** tab, click **Service Requests**.

> ⓘ Note: To create a service request, you must have a valid support agreement. For details about either an account or obtaining a valid support agreement, contact a sales representative. To find the details of a service request, in the `Service Request Number` field, type the service request number, and then click the right arrow.

To review an open service request:

1. Go to https://www.dell.com/support.
2. On the **Support** tab, click **Service Requests**.
3. On the **Service Requests** page, under **Manage Your Service Requests**, click **View All Dell Service Requests**.

Online communities

For peer contacts, conversations, and content on product support and solutions, go to the Community Network https://community.emc.com. Interactively engage with customers, partners, and certified professionals online.

How to provide feedback

Feedback helps to improve the accuracy, organization, and overall quality of publications. You can send feedback to DPAD.Doc.Feedback@emc.com.

CHAPTER 1

DD Boost Features and Environment

This chapter includes the following topics:

DD Boost integration features

The NetWorker integration with Data Domain systems uses DD Boost deduplication devices.

The following integration features are available:

- DD Boost and data deduplication
- Data Domain cloud tier
- Data Domain high availability support
- Client Direct data handling
- DD Boost device storage
- DD Boost synthetic full backups
- DD Boost in-flight encryption
- DD Boost clone operations
- NetWorker Management Console (NMC) management of DD Boost operations
- DD Retention Lock

DD Boost and data deduplication

NetWorker client software uses DD Boost to integrate with DD Boost logical storage devices on Data Domain systems, and perform data deduplication backups. Data deduplication is a type of data compression that removes duplicate information to reduce the amount of backup data that is sent to the storage devices. The reduction in data that is sent to the devices reduces the bandwidth that is required for the data transport.

DD Boost can run up to 60 concurrent sessions or save streams on each DD Boost device for backup and recovery. Running concurrent sessions reduces the number of required devices and reduces the impact on the performance and maintenance of the Data Domain system. The resulting performance gain provides an advantage over conventional advanced file type device (AFTD) or virtual tape library (VTL) interfaces that do not handle these concurrent high session rates.

During recovery to a NetWorker client, the Data Domain system converts the stored data to its original non-deduplicated state.

Data Domain Cloud Tier

The Data Domain Cloud Tier (DD Cloud Tier) is a long term data retention solution that enables the movement of data from an Data Domain Active Tier (DD Active Tier) device to a DD Cloud Tier device, and then to an external Cloud Provider.

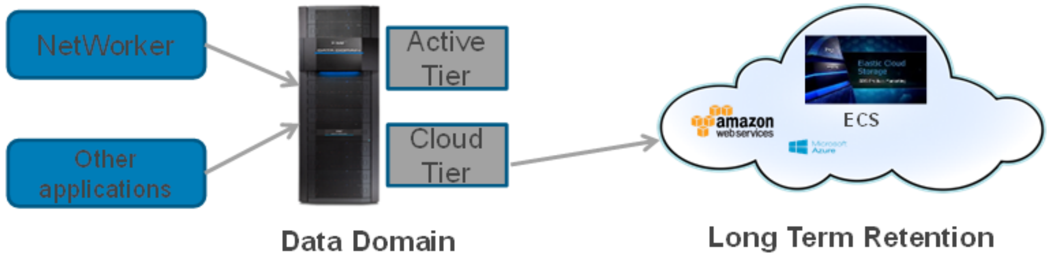
The NetWorker integration with the DD Cloud Tier provides a Data Protection Administrator with the ability to perform the following functions:

- Ability to clone data from a DD Active Tier device to a DD Cloud Tier device.
- Track individual client data that is stored in the cloud or on-premise.
- Recover data to a client from the cloud, including FLR/GLR recoveries.

NetWorker supports the following Cloud services, for long term retention in this release: Amazon web services (AWS), Elastic Cloud Storage™ (ECS™), and Microsoft® Azure®

The following diagram provides an overview of the DD Cloud Tier solution.

Figure 1 DD Cloud Tier solution



Data Domain high availability support

NetWorker 18.1 and later supports highly available Data Domain systems.

To configure alerts for the following Data Domain high availability events, during Data Domain device setup, select the following options from the **Device Configuration Wizard** > **SNMP Monitoring Options** page:

- **HA Setup Degraded**
- **HA Setup Offline**
- **HA Setup Out-of-Sync**

When a highly available Data Domain system fails over to its standby highly available Data Domain system, NMC displays event messages. All in-progress NetWorker operations including backup, clone, and recover operations are unaffected, except for a temporary freeze of operations for a few minutes. However, during unusually long freezes, for example over ten minutes, some NetWorker operations might fail but are automatically retried. Some failed NetWorker operations might require a manual restart.

If interrupted by a failover NFS, VTL, and CIFS jobs fail. You must configure NetWorker policies to restart or resume the failed jobs. You can manually restart the failed jobs as soon as the failover completes. The failed jobs will not restart or resume on their own. You must ensure that the VTL devices are visible and detected by NetWorker on the secondary Data Domain system before a backup is triggered.

ⓘ **Note:** To view events in NMC, clear all alerts on the Data Domain system. For example, in the Data Domain UI, select **Alerts** > **Current Alerts** > **Select All** > **Clear**.

Client Direct data handling

The Client Direct feature enables clients that have a direct network connection or a DD Boost over Fibre Channel (DFC) connection to the Data Domain system to send and receive data directly to Data Domain AFTD and DD Boost devices. Client Direct supports multiple concurrent backup and restore operations that bypass the NetWorker storage node, which eliminates a potential bottleneck. The storage node manages the devices that the clients use but does not handle the backup data. Client Direct was previously known as Direct File Access (DFA).

When a connection is available, by default NetWorker enables Client Direct and also uses Client Direct to recover duplicated backups that NetWorker performed by using a storage node.

DD Boost device storage

A Data Domain system stores deduplicated NetWorker backup data on DD Boost storage devices on the Data Domain system. The NetWorker server, storage nodes, and Client Direct clients can all access the DD Boost devices. The DD Boost devices appear as folders that reside in storage unit (SU) partitions.

Secure multi-tenancy

NetWorker supports DD Boost devices in secure multi-tenancy (SMT) storage on Data Domain systems. SMT enables service providers to isolate tenant users on a Data Domain system. A global storage administrator assigns or creates a tenant unit (TU) for each tenant user. Tenant users (for example, backup administrators) must use a DD Boost username and password to create the secure storage units (SUs) that the DD Boost devices use to store data.

Retention tier storage

For long-term retention of deduplicated backup data, the Data Domain Extended Retention software option extends the Data Domain storage structure with internal tiers.

Use Data Domain operations to migrate the data from the active tier to the retention tier. The active tier does not require additional capacity licensing.

On an Extended Retention-enabled Data Domain system, the NetWorker software interacts with the active tier only and is not aware of any migration activity between the internal storage tiers. This model of a Data Domain system can support mixed environments that may include DD Boost devices, VTL, and CIFS or NFS AFTD disk configurations.

DD Boost Synthetic Full backups

The NetWorker Synthetic Full backup feature is an efficient way to create full backups by combining existing full and incremental backups. This feature integrates the NetWorker Synthetic Full backup feature and the Data Domain virtual-synthetics feature. NetWorker creates the Synthetic full backups directly on the DD Boost devices. By default, both the NetWorker software and the Data Domain system are configured to enable DD Boost synthetic full backups.

To perform a Synthetic Full Backup from NetWorker, change the backup level to **Incremental Synthetic Full** using the NMC **NetWorker Administration** window's **Policy Action Wizard**, or right-click a policy within the **NetWorker Administration Protection** window and select **Properties**.

The *NetWorker Administration Guide* provides more details about the Synthetic Full feature.

DD Retention Lock

The Data Domain Retention Lock (DD Retention Lock) feature within NetWorker allows you to efficiently manage and store different types of data backed up by NetWorker to a single Data Domain system by securely locking the data on that system, preventing accidental deletion of save sets.

When you enable a device with DD Retention lock and DD Retention lock period is set in data protection policy action, the save sets backed up by the NetWorker policy cannot be overwritten, modified, or deleted for the duration of the retention period, up to a maximum of 70 years. Additionally, the device cannot be removed or relabeled at any time during the retention period, though the device that contains the Retention Lock save sets can be mounted and unmounted. The secure locking of data occurs at an individual file level, and locked files can co-exist with unlocked files on the same Data Domain system.

With DD Retention Lock, you can set the retention time to meet the requirements driven by governance policies. The **DD Retention Lock Time** specified at the save set level must fall within the range of the minimum and maximum retention times configured on the DD Boost Mtree during device creation. The Retention lock modes are Compliance lock mode and Governance lock mode. Governance mode is supported from NetWorker 9.2 onwards. Compliance mode is supported from NetWorker 18.1 onwards.

You can enable DD Retention Lock on the DD Boost Mtree during device configuration, as described in the section Configuring DD Boost devices with the NMC Device Configuration wizard, or by modifying the device properties after configuration, as described in the section Configuring a DD Boost device manually. If using the NMC **Device Configuration** wizard for the first instance of Data Domain device configuration, ensure that you populate the Data Domain device management credentials (Management host, Management user name, management password and management port).

When you enable DD Retention Lock at the device level, you must additionally set Retention Lock period to the data protection policy action so that data is backed up with Retention Lock set. The section Creating a traditional backup action provides more information.

After successful backup, save set queries in the **Media** window of **NetWorker Administration** displays **DD Retention Lock Period** and **DD Retention Lock Type** columns to indicate which save sets have Retention Lock enabled and provide the Retention Lock expiry date and time. If these columns are not initially visible, you can customize the view to include this information. This information is also available within the **NMC Enterprise Reports** window, under **Policy Statistics** > **Save Set Details**. Similarly, if these columns are not initially visible, you can customize the view to include this information.

Requirements

Review the following requirements for enabling DD Retention Lock:

- The NetWorker Server and storage node version must be NetWorker 19.2.
- The minimum DDOS version required when using the DD Retention Lock feature is DDOS 6.0. The minimum DD Boost version is 3.4.
- Workflows that contain Data Domain Retention Lock enabled save sets require a separate destination pool. The pool cannot contain a mixture of Retention Lock and non-Retention Lock enabled Data Domain devices.
- The Data Domain devices storing primary and cloned backups with DD Retention Lock enabled cannot be labelled or deleted. Disk space utilization issues will result on the Data Domain system.
- The Data Domain Retention Lock feature is only supported only for DD Boost instances.
- All configuration changes must be performed from NetWorker. Any configuration changes from the Data Domain device will not be reflected in NetWorker.

DD Boost in-flight encryption

NetWorker enables DD Boost clients to have in-flight data encryption with a Data Domain system running DDOS 5.5 or later over a WAN connection. To use this feature, you must configure the Data Domain system to use medium-strength or high-strength TLS encryption. The configuration is transparent to NetWorker.

The Data Domain documentation provides more information about DD Boost in-flight encryption.

DD Boost clone operations

For added protection and efficient disaster recovery, you can create a clone of the backup data that is stored on DD Boost devices, and then copy the clone data to remote offsite storage. To use the NetWorker clone feature, add a clone action to a workflow in a data protection policy. The clone action generates information that NetWorker stores in the client file index and media database to enable data recovery. The retention policy that is assigned to the clone action defines the length of time that NetWorker retains the data. All data movement for NetWorker clone operations must use Fibre Channel (DFC) or IP network connectivity.

The following clone operations are supported:

- NetWorker clone-controlled replication (CCR or enhanced cloning) operations. This operation replicates data from a DD Boost device to another DD Boost device at a different location.

CCR preserves the deduplicated data format and minimizes bandwidth usage between the Data Domain systems.

- Clone to native format operations. This operation clones data from DD Boost storage to conventional storage media, such as disk or tape. This operation reverts the data to the native non-deduplicated format, to enable recovery from a conventional disk device or tape device.

NMC management of DD Boost operations

You can use the NetWorker Management Console (NMC) to efficiently configure, monitor, and generate reports for DD Boost devices. The NMC server and the NetWorker server must have network access to each managed Data Domain system.

The NMC Device Configuration Wizard simplifies the configuration of DD Boost storage devices, backup clients, storage pools, volume label operations, and save set clone operations.

Feature not supported by the integration

Native Data Domain directory replication (MTree replication) does not fully support DD Boost devices, which are rendered as read-only directories. Native Data Domain replication considerations on page 128 provides details.

Data Domain network environment

This section describes various components in a NetWorker with Data Domain network environment.

FC and IP network connectivity

DD Boost devices support data transport over Fibre Channel (FC) and Ethernet IP (IPv6 and IPv4) network connections for backup and recovery operations with Data Domain systems.

NetWorker supports DD Boost devices on IPv6 networks and Data Domain systems support IPv6 network usage with DHCP, DNS, and DDNS Internet services. The Dell *EMC Data Domain Operating System Administration Guide* provides configuration details.

When you use DFC for data transport, verify the following requirements:

- The NetWorker server also requires IP connections, to communicate with all the hosts that are involved in DD Boost operations and for data transport during recovery and clone-controlled replication operations.
- Client Direct backup with DFC is not supported for 32-bit Linux NetWorker clients that are installed on 64-bit Linux systems. The backup reverts to a storage node backup.
- For DFC to work, the encryption strength for the client "*" on the DD OS, verify that the option is set to **None**. By default, the setting is set to **High**.

Data Domain storage system

A Data Domain system can store deduplicated backup data or clone data on DD Boost devices, and supports mixed environments that may include DD Boost devices, VTLs, and CIFS or NFS AFTD disk configurations. The Data Domain system may require additional licenses for the DD Boost functionality.

The *NetWorker E-LAB Navigator* provides compatibility information.

NetWorker client

A NetWorker client is a supported host whose data requires protection. The NetWorker client software includes an integrated DD Boost plug-in. The NMC server, NetWorker server, and NetWorker storage nodes are also NetWorker clients.

NetWorker clients that use Client Direct deduplication must have direct network access to the Data Domain system, which stores the data. By default, NetWorker enables Client Direct in the properties of the Client resource.

Client Direct with FC connectivity to DD Boost devices requires NetWorker client 8.1 or later.

The *NetWorker E-LAB Navigator* provides information on supported releases.

NetWorker Server

The NetWorker Server is a collection of processes and programs that are installed on a host that performs NetWorker services. The NetWorker Server also acts as a storage node and can control multiple remote storage nodes.

NMC Server

The NetWorker Management Console (NMC) server or Console server is a Java-based application and database server. The NMC Server manages all NetWorker Servers and Clients. The NMC Server provides reporting and monitoring capabilities for all NetWorker Servers and Clients in the environment. The NMC Server relies on the NetWorker Authentication Service for user account authentication.

NetWorker storage node

NetWorker storage nodes manage DD Boost and other storage devices. If a NetWorker client does not use Client Direct, the NetWorker storage node deduplicates the backup data, then sends the deduplicated data to the DD Boost devices.

Install the same version, including the service pack of the NetWorker storage node software, on each host in the datazone that stores backup or clone data on DD Boost devices. Also, ensure that the storage node is at the same version as the NetWorker Server.

NetWorker application modules

NetWorker supports Client Direct deduplication backup and recovery on clients with supported NetWorker application modules (for example, NetWorker Module for Databases and Applications, NetWorker Module for Microsoft Applications, and NetWorker Module for SAP). The clients must have direct network access or Fibre Channel access to the Data Domain system. The release notes for the application module provide details.

Licensing for Data Domain systems

The following types of licensing models can enable the NetWorker server to interact with a Data Domain system:

- The Dell EMC Licensing Solution with capacity entitlement, introduced in NetWorker 9.0, which uses an Dell EMC License Server and a license file.
- Traditional Licensing, which uses individual enabler codes to license features. NetWorker requires only a single enabler to support multiple interfaces and multiple network identities for Data Domain systems.

- Capacity Licensing from NetWorker 8.2.x and previous releases, which licenses the datazone by using capacity-based enabler codes.

The *NetWorker Licensing Guide* provides licensing details.

Traditional licensing for Data Domain systems

If you use traditional licensing, a new installation of the NetWorker server software enables you to evaluate all the features for 30 days, including the Data Domain features, without the use of an enabler (license key). To extend this evaluation period by 15 additional days, type the word **`grace`** in the **Auth code** field of the NetWorker server evaluation license before the end of the 90-day period. After the evaluation period ends, you cannot perform a backup unless you install permanent license enabler codes.

Data Domain licenses

Enable either the Data Domain system or the Data Domain system with Extended Retention software by using the following licenses for DD Boost operations:

- DDBOOST license
- To use CCR, a REPLICATION license
- To use Cloud Tier, a CLOUDTIER-CAPACITY license
- To use Retention Lock with Governance Mode, a RETENTION_LOCK_GOVERNANCE license
- To use Retention Lock with Compliance Mode, a RETENTION_LOCK_COMPLIANCE license

To generate a list of the enabled licenses on the Data Domain system, type the `license show` command. The output displays DDBOOST when a DD Boost license is installed, and REPLICATION when a replication license is installed. Configuring the Data Domain system for DD Boost by using the CLI on page 48 provides details.

For license inquiries, go to the Data Domain portal for service and support at https://support.emc.com.

CHAPTER 2

Planning and Practices

This chapter includes the following topics:

DD Boost storage characteristics

NetWorker integrates with Data Domain systems by storing backup data on DD Boost devices.

The *NetWorker E-LAB Navigator* provides information about supported releases.

DD Boost storage structures and limits

DD Boost devices use a folder structure on the Data Domain system that has the following characteristics:

- The Data Domain storage consists of separate logical partitions called storage units (SUs) or managed trees (MTrees).
- By default, the NetWorker Device Configuration Wizard creates one SU for each NetWorker datazone. The wizard names the SU after the short hostname of the NetWorker server.
- You can define up to 99 active SUs on a Data Domain system, depending on the specific model and DDOS code. Not all Data Domain systems support 99 active SUs.
- DD Boost devices appears as subfolders within the SU folder.
- You can associate each DD Boost device with only one NetWorker storage volume. However, a single NetWorker volume can share multiple DD Boost devices, which in some environments can improve performance.
- You must use DD Boost credentials to create the SUs and the DD Boost devices, and to enable secure multi-tenancy (SMT) access to the DD Boost devices.
- Avoid changing the user of a device; the new user will not have permission to the files and directories created by the previous user and cannot re-label the volume; create a device for the new user.
- For SMT, NetWorker supports up to 512 DD Boost devices on each SU. Otherwise, there is no limit on the number of DD Boost devices that you can create. For best performance, use fewer devices and more backup sessions on each device.
- Data Domain MTree quotas manage the usable capacity of SUs. When an MTree reaches the defined quota, any running DD Boost backup operation terminates.

SMT structure

For SMT storage, a global storage administrator isolates DD Boost users, for example backup administrators, by assigning them to tenant units (TUs). A TU cannot span Data Domain systems. You can assign a DD Boost user to only one TU, but you can assign multiple DD Boost users to the same TU. Each DD Boost user can create SUs within the assigned TU only. Security is enforced at the TU level by the DD Boost user assignment on the Data Domain system, and at the SU level by the DD Boost credentials.

For example:

Tenant 1: bob, tu1, su1

Tenant 2: joe, tu2, su2

Tenant 3: sue, tu2, su3

DD Boost volume sharing

Multiple DD Boost devices, specified by different names or aliases, can concurrently share a single NetWorker storage volume.

Each DD Boost device operates with a single NetWorker storage volume and you must specify each device by the device access pathname.

- Each DD Boost device operates with a single NetWorker storage volume and you must specify each device by its device access pathname.
- You can create multiple devices with the same device access pathname, provided that you assign each device a different name, as an alias. You can use the different device aliases, for example, to manage different client hosts that share the same volume.

Configuring a DD Boost device manually on page 89 provides details on device access information.

DD Boost performance

DD Boost devices use multiple concurrent `nsrmmd` (media mover) processes per device and each `nsrmmd` process uses multiple concurrent save sessions (streams or threads). This reduces the performance and maintenance impacts on the Data Domain system.

Balance the session load among the available DD Boost devices so that new sessions attach to devices with the least load. To enable best performance, you can adjust the **Target Sessions**, **Max Sessions**, and **Max nsrmmd Count** attributes assigned to the Device resource on the NetWorker server.

Configuring a DD Boost device manually on page 89 provides details on session settings.

The Data Domain documentation provides additional details on save sessions and performance.

Memory requirements for DD Boost

The physical memory requirement for a NetWorker storage node and a Client Direct client depends on the peak usage of the DD Boost devices.

Ensure the following memory requirements:

- A storage node host that manages DD Boost devices with other typical devices and typical services must have a minimum of 8 GB of RAM.
- A DD Boost client requires a minimum of 4 GB of RAM at the time of backup to ensure the best performance for Client Direct backups.

Devices in mixed device environments

A Data Domain system can support mixed NetWorker environments, which can include DD Boost devices, VTLs, and CIFS or NFS AFTD disk configurations. Each different storage environment must use a different interface connection. Use a NIC for IP data transport and an FC port for SAN data transport. You can use the NetWorker clone process over an IP connection to migrate legacy data that is stored in these traditional storage environments to DD Boost devices.

DD Boost devices and media pools

Use media pools to send client backups or clones of the backup data to specific storage devices. You must configure pools for DD Boost devices with the following important consideration.

A pool that contains the DD Boost devices must not contain any other type of storage media and must not contain devices on more than one Data Domain system.

This practice ensures an optimal backup window and deduplication ratio with the least amount of interference. When you store each backup on a single Data Domain system, you simplify recovery and Data Domain file replication.

Periodically review and remove unused pools that are no longer relevant to the storage environment.

Reclaiming expired storage space

When a backup on a Data Domain system reaches the retention expiry date, all references to the data become invalid. However, unlike conventional storage systems, the Data Domain system does not immediately free up disk space on the device because other existing backups or other clients may continue to have deduplication references to the same data.

For example, the deletion of 1 GB of data, even of unique data from a NetWorker perspective, does not mean that 1 GB of space is immediately available on the Data Domain system.

The DD OS `filesys show space` or `df` command shows the data that is eligible for deletion under the **Cleanable GiB** column.

The Data Domain system periodically reviews deduplication references and storage space and performs a cleanup. By default, these cleanups occur weekly.

ⓘ Note: If a DD Boost device becomes full during a backup, the backup immediately fails. The device does not pause or wait for space to become available.

The DD OS `filesys clean` command describes all the available options that you can use to reclaim and recycle expired NetWorker save sets and other redundant or expired data.

Removing a DD Boost device

You must use special procedures to remove DD Boost devices.

Deleting an AFTD or a DD Boost device on page 97 provides details.

DD Boost devices on Extended Retention systems

You can use SU folders or MTrees and DD Boost devices on Data Domain Extended Retention systems, similar to those on standard Data Domain systems, with the considerations described in this section.

The Data Domain documentation provides details on Data Domain Extended Retention features.

Active and extended retention tier structure

On Data Domain Extended Retention systems, you can store data in two tiers of SUs, an active tier and an extended retention tier.

Data Domain places all incoming data first in the active file system tier, which is for short-term data storage and is similar to standard Data Domain systems. You can use the active tier for client backups, provided that you apply appropriate data movement and data retention policies. It is recommended that you create separate SUs for backup operations. You can move data from the active tier to the archive tier, based on data movement policies that you apply at the SU level.

DD OS supports up to 14 active and 99 defined SUs with the Extended Retention software feature. NetWorker does not limit the number of DD Boost devices that you can create on the system.

Data movement between tiers

Each SU has a single data movement policy that applies to all the devices that the SU manages within the corresponding NetWorker datazone.

You can create a Data Domain SU data movement policy to specify when the data moves from devices in the active tier to devices in the archive tier. Typically, you would not move data to the archive tier for less than 30 days retention. The policy and movements are internal to the Data Domain Extended Retention system, and the NetWorker software has no awareness of the operations.

You can assign alternative data movement policies to the client data by using additional SUs, created by NMC or `nsradmin`, for moving data from one tier to another. For example, you can store data to different archive DD Boost devices in separate SUs with different archive policies. Also, you can move data within the same Data Domain Extended Retention system by using CCR.

To use CCR on the same Data Domain system that includes the Extended Retention software feature, you must replicate between two different SUs. You can apply different retention policies to manage the data efficiently.

Data Domain Cloud Tier system requirements

Data Domain systems that support the Extended Retention Tier and Data Domain Virtual Edition (DDVE) support Cloud Tier.

To use Data Domain Cloud Tier with a DDVE, ensure that the appliance meets the following minimum requirements:

- 16 TB DDVE
  - DD OS 6.0
  - DDVE— 4 CPUs, 32 GB memory, 200 GB Active Tier disk, 500 GB Cloud Tier disk
- 64 TB DDVE
  - DD OS 6.0
  - DDVE— 8 CPUs, 60 GB memory, 200 GB Active Tier disk, 500 GB Cloud Tier disk
- 96 TB DDVE
  - DD OS 6.0
  - DDVE— 8 CPUs, 80 GB memory, 200 GB Active Tier disk, 500 GB Cloud Tier disk

Network requirements

DD Boost devices support data transport over both Ethernet IP networks and FC SAN environments for both data backup and data recovery operations.

The NetWorker server requires Ethernet IP connections to control all hosts involved in the DD Boost operations.

Ethernet IP support

DD Boost devices do not distinguish between different TCP/IP network types (LAN, WAN, or MAN) and can successfully operate in a network where packet loss is strictly 0% and latency is less than 20ms. Variations of IP network connections can improve data throughput, depending on the Data Domain system model.

It is recommended to use a minimum of two separate IP network connections to the Data Domain system. One is used for administration and the other is used for data backup.

Aggregated multiple connections can further improve data throughput for the Data Domain system. For example, you can use multiple 1 GbE connections for dedicated storage nodes and storage devices. Connections for 10 GbE are also available and you can use these instead of or with 1 GbE links.

You can configure two basic IP interfaces:

- Dedicated 1 GbE data connection from the storage node directly to the Data Domain system. This connection provides a private, high-bandwidth data connection and avoids the latency and

complexity of a shared IP connection. You also require a separate conventional IP connection for administration and NetWorker Console access.
The *Data Domain Operating System Administration Guide* provides details on network support.

- Two or more NICs on the Data Domain system with 1 GbE or 10 GbE connections, which are aggregated together by using the Data Domain `ifgroup` command. This grouping provides increased data capacity and can improve resiliency. The Data Domain system provides automatic Advanced Load Balancing and Link Failover for NIC connections.

  ⓘ **Note:** NetWorker supports ifgroups for replication. Do not use aggregated connections for replication operations.

  The *Data Domain Boost for Open Storage Administration Guide* describes the benefits, limitations, and examples of using ifgroups, which apply to NetWorker.

Fibre Channel support

NetWorker supports data backup and recovery operations to DD Boost devices over Fibre Channel (DFC or FC) connections, which are configured as a SAN, as follows:

- The NetWorker storage nodes and all Client Direct clients must have FC SAN network access to the Data Domain systems that have FC-enabled DD Boost devices.
- The environment must have an Ethernet IP network. The NetWorker server uses IP connections to communicate with the clients, storage nodes, and the Data Domain system. DD Boost devices that are involved in CCR operations must have IP connectivity for the data transport.
- FC-enabled NetWorker clients must run on a supported Windows, Linux, HP-UX, AIX, or Solaris operating system. HP-UX systems must have minimum versions of NetWorker 9.0.1 clients and storage nodes. AIX systems must use NetWorker 9.0.1 clients and storage nodes. Supported Solaris versions on a client are Solaris 10 and 11 on SPARC with x86 architectures. Solaris uses SCSI generic device driver, sgen. The sgen driver is included in the Solaris installation. The *NetWorker E-LAB Navigator* and the *Dell EMC Data Domain Boost Compatibility Guide* provide details.

  ⓘ **Note:** On AIX, DD Boost-over-FC requires a device driver. The AIX Installation Chapter in the *NetWorker Installation Guide* provides more details.

- The NetWorker clients and NetWorker storage nodes must run NetWorker NetWorker 9.0.1 or later software.
- All hosts that use FC must have an HBA card with at least 4 Gbps bandwidth capacity and must devote an initiator port on each card to FC for DD Boost devices. You should configure Access groups. The *DD OS Administration Guide* provides details.
- FC-enabled DD Boost devices support Client Direct backup and restore over FC, provided that you have enabled the clients with FC connections and settings.
- Data Domain systems support the coexistence of FC-enabled DD Boost devices together with VTL devices on the same Data Domain system. However, the FC-enabled DD Boost devices must not share an initiator with VTL devices on the same Data Domain system.
- CCR is supported between FC-enabled DD Boost devices provided that there is IP connectivity between the Data Domain systems. CCR is not supported over a Fibre Channel network.

You can convert an existing DD Boost device from IP to FC connectivity and settings without losing the stored data. You can restore the data to FC-enabled Client Direct clients through their FC connection, and to IP-only clients through the storage node. Converting DD Boost devices from IP to FC connectivity on page 182 provides details.

The NetWorker server can migrate legacy backup data stored on a VTL or tape device to an FC-enabled DD Boost device. You can create a clone pool for this migration. Considerations for migrating legacy save sets provides details.

The *NetWorker E-LAB Navigator* provides the latest details of supported versions.

Configuring DD Boost-over-FC Service

Before you begin

In order to support the DD Boost-over-FC service, it is necessary to install supported Fibre Channel Target HBAs into the system. (See also the *Data Domain Operating System Command Reference Guide* and *Administration Guide* for information about `scsitarget` as a related command that may be helpful in managing the SCSI target subsystem.)

> **Note:**
>
> - Windows, Linux, HP-UX, AIX, and Solaris client environments are supported.
> - Beginning with DD Boost 3.3 and DD OS 6.0, you do not need a device driver; you can enable DD Boost-over-FC by creating a ddboost fc group; see Step 3 in the following procedure.
> - To enable DD Boost-over-FC on clients running AIX, you can also install the AIX DDdfc device driver.

Ensure that the client's HBA ports and the Data Domain system's endpoints are defined and that appropriate zoning has been done if you are connecting through a Fibre Channel switch.

Procedure

1. Enable the DD Boost-over-FC service:

   ```
   # ddboost option set fc enabled
   ```

2. Optional: set the DFC-server-name:

   ```
   # ddboost fc dfc-server-name set <server-name>
   ```

   Alternatively, accept the default, which has the format `DFC-<base hostname>`. The hostname cannot be the fully-qualified domain name.

   A valid DFC server name consists of one or more of the following characters:

   - lowercase letters (“a”–“z”)
   - upper-case letters (“A”–“Z”)
   - digits (“0”–“9”)
   - underscore (“_”)
   - dash (“–”)

   > **Note:** The dot or period character (“.”) is not valid within a `dfc-server-name`; this precludes using the fully qualified domain name of a Data Domain system as its `dfc-server-name`.

   > **Note:** Similar to IP hostnames, the `dfc-server-name` is not case-sensitive. Multiple Data Domain sytems accessible by the same clients using DDBoost-over-FC should be configured without case-sensitive `dfc-server-name`.

3. Create a SCSI target access group:

   ```
   # ddboost fc group create <group-name>
   ```

   Example:

   ```
   # ddboost fc group create lab_group
   ```

4. To display the available list of scsitarget endpoints, enter:

   ```
   # scsitarget endpoint show list
   Endpoint         System Address   Transport      Enabled   Status
   ```

```
-------------    --------------    ------------    -------    ------
endpoint-fc-0         6a           FibreChannel    Yes        Online
endpoint-fc-1         6b           FibreChannel    Yes        Online
-------------    --------------    ------------    -------    ------
```

5. Indicate which endpoints to include in the group:

   ```
   # ddboost fc group add <group-name> device-set
   count count endpoint endpoint-list [disk <disk-name>]
   ```

   Note: The disk option in the previous example is optional and supported only if the client is AIX.

   Example:

   ```
   # ddboost fc group add lab_group device-set count 8 endpoint 6a
   ```

6. Verify that initiators are present. To view a list of initiators seen by the Data Domain system:

   ```
   # scsitarget initiator show list
   ```

7. Add initiators to the SCSI target access group:

   ```
   # ddboost fc group add group-name initiator initiator-spec
   ```

   Example:

   ```
   # ddboost fc group add lab_group initiator "initiator-15,initiator-16"
   ```

Sizing DD Boost-over-FC device-set

The protection system advertises one or more "DFC devices" of type Processor, which the DD Boost library uses to communicate with the DD Boost-over-FC service. On the protection system, access to these DFC devices is granted to one or more initiators by adding the initiators to a ddboost-type scsitarget access group:

```
# ddboost fc group add lab_group initiator "initiator-15,initiator-16"
```

The number of DFC devices advertised to the initiator is controlled by configuring the device-set of the scsitarget access group:

```
# ddboost fc group modify lab_group device-set count 4
```

The maximum number of supported DFC devices per protection system is 64. You can have the same devices in multiple groups, but each group is limited to 64 devices.

Note: AIX DDdfc drivers support 128 devices. However, if you use the `disk` option with the `ddboost fc add` command, this limitation is removed.

Because the DFC client sees each path to the protection system as a separate device, more paths and more DFC devices mean better performance for constrained clients such as AIX, Windows, and Solaris.

So, how many DFC devices should be advertised to initiators on a given backup server? The answer depends upon several factors:

1. Is the backup server queue-depth constrained?
   Windows platforms are considered “queue-depth constrained,” because the Windows SCSI Pass-Through Interface mechanism will only conduct 1 SCSI request at a time through each of its generic SCSI devices. This impacts the performance of the DD Boost-over FC solution, if multiple connections (for example, backup jobs) are trying to use the same generic SCSI device. So, for Windows platforms running more than one job, it is useful to advertise multiple DFC devices.

Contrast this with the behavior of the Linux SCSI Generic driver, which imposes no such restriction. Linux is not considered "queue-depth constrained," so it is sufficient to simply advertise one DFC device to initiators on Linux systems.

2. Number of physical paths between backup server and protection system
For each advertised DFC device, the backup server operating system will create *n* generic SCSI devices, one for each physical path through which the backup server OS can access the device.

   For example, if:

   - Backup server has 2 initiator HBA ports (A and B)
   - Protection System has 2 FC target endpoints (C and D)
   - Fibre Channel Fabric zoning is configured such that both initiator HBA ports can access both FC target endpoints

   then the backup server OS will see each device through four physical paths:

   A -> C
   A -> D
   B -> C
   B -> D

   and will create 4 generic SCSI devices for each advertised DFC device.

   For a Windows backup server (with its queue-depth=1 limitation), this allows up to 4 simultaneous SCSI requests to the protection system, even with only one DFC device advertised.

Sizing calculation

The following calculation may be used to determine the number of DFC devices to advertise on the Data Domain system and to the initiators on a given media server. Dell EMC recommends that the same number of DFC devices be advertised to all initiators on the same media server.

The following calculation may be used to determine the number of DFC devices to advertise on the Data Domain system and to the initiators on a given backup server. It is recommended that the same number of DFC devices be advertised to all initiators on the same storage nodes.

On the Data Domain System

The Data Domain system imposes a limit on the number of simultaneous requests to a single DFC SCSI device. Because of this limit, the number of devices advertised needs to be tuned depending on the maximum number of simultaneous jobs to the system at any given time. In general, the larger the number of jobs expected from media servers using DD Boost over FC, the higher the number of devices advertised.

The Data Domain system imposes a limit on the number of simultaneous requests to a single DFC SCSI device. Because of this limit, the number of devices advertised needs to be tuned depending on the maximum number of simultaneous jobs to the system at any given time. In general, the larger the number of jobs expected from storage nodes using DD Boost over FC, the higher the number of devices advertised.

Let J be the maximum number of simultaneous jobs running using DFC, to the Data Domain System at any given time.

Let C be the maximum number of connections per job:

- 3 for Data Domain Extended Retention Systems
- 1 for other types Data Domain systems

Let D be the DFC device count. All device groups on the server and storage node must be configured with "D" devices.

Calculate:

- Maximum simultaneous connections to the DD system, using DFC, from ALL media servers:
  - S = J * C
  - DFC Device Count (D) = minimum (64, 2*(S/128)), rounded up to a whole number.
- Maximum simultaneous connections to the DD system, using DFC, from ALL storage nodes:
  - S = J * C
  - DFC Device Count (D) = minimum (64, 2*(S/128)), rounded up to a whole number.

Example:

To calculate the max simultaneous connections to the Data Domain system by using DFC from ALL media servers, assume:

- 8 media/master servers, single Data Domain systems, each server running a maximum of 50 jobs at any given time.
  Therefore, J = 8 * 50 = 400

  C = 1 (single Data Domain system)

  S= J * C

  S= 400 * 1

  S= 400
- 8 storage nodes, single Data Domain systems, each server running a maximum of 50 jobs at any given time.
  Therefore, J = 8 * 50 = 400

  C = 1 (single Data Domain system)

  S = J * C = 400

  D = 2 * 400 / 128 = 6.25. Round up to 7.
- Therefore, all DFC groups on the Data Domain system must be configured with 7 devices.

Assume:

- 8 media servers, DD Extended Retention systems, each server running a maximum of 30 jobs at any given time.
- 8 storage nodes, DD Extended Retention systems, each server running a maximum of 30 jobs at any given time.
- Here, J = 8 * 30 = 240, C = 3 (DD Extended Retention system), S = J * C = 720, D = 2 * 720 / 128 = 11.25, round up to 12.
- Therefore, all DFC groups on the DD system must be configured with 12 devices.

Linux

The number of DFC devices advertised on the Data Domain system using the calculations listed above in *On the Data Domain System* is sufficient for Linux backup servers. No additional configuration is required. Linux storage nodes are not queue-depth constrained, so many connections can share the same DFC generic SCSI device with no performance impact.

Windows

The Data Domain server path management logic spreads out connections across available logical paths (Initiator, Target Endpoint, DFC Device). We want to configure enough DFC devices such that each connection uses its own generic SCSI device (logical path) on the backup server, with a max DFC device count of 64.

Let X = the number of DFC devices configured on the Data Domain system (from *On the Data Domain System*). Let P = number of physical paths between backup server and Data Domain system. Let J = maximum number of simultaneous jobs, and let C = maximum number of connections per job:

– 3 for DD Extended Retention systems – 1 for other types of Data Domain systems

Calculate:

- Maximum simultaneous connections from storage node S = J * C, DFC device count D = minimum((S/P), X), round up, up to a maximum of 64.

Note that if the value of D is greater than X, then it is sufficient to configure D devices, but only for the access group(s) with Windows clients.

Examples:

Assume:

- 4 physical paths between the storage node and Data Domain system, 30 maximum jobs, DD Extended Retention system
- In this case, X = 25, P = 4, J = 30, and C = 3
- Maximum simultaneous connections from backup server S = (J * C) = 90
- DFC device count D = (90/4, 25) = 25

So, the Data Domain system should be configured to advertise 25 devices to each initiator on the storage node.

Assume:

- 2 physical paths between the backup server and Data Domain system, 50 maximum jobs, single Data Domain system
- In this case, X=18, P = 2, J = 40, C = 1
- Maximum simultaneous connections from backup server S = (J * C) = 40
- DFC device count D = max(40/2, 18) = 20

So, the Data Domain system should be configured to advertise 20 devices to each initiator on the storage node.

Note that since the value of D (20) is greater than the value of X (18), it is sufficient to configure two devices only for the DFC access group with Windows clients.

Firewall requirements

Regardless of the network connections that are used, communication through a firewall requires the use of specific ports and specific protocols to perform backup, monitoring, and replication operations across sites.

The following table lists the required firewall ports, which you must open between the Data Domain system, the NetWorker server, and the NMC server.

Table 3 Firewall ports for DD Boost

Port	Protocol	Purpose	Source	Destination
111	TCP/UDP	Portmapper	• All DD Boost clients • DD Replication Source	• Data Domain backup target • Data Domain Replication target
161	TCP	For the NMC	• NMC Server	• Data Domain backup target

Table 3 Firewall ports for DD Boost (continued)

Port	Protocol	Purpose	Source	Destination
		server to query for alerts and statistics		• Data domain Replication target
162	TCP	SNMPTRAP for the NMC server to monitor status and events	• NMC Server	• Data Domain backup target • Data Domain Replication target
2049	TCP	NFS	• DD Boost Clients	• Data Domain backup target
2049	TCP	DDBoost	• NMC Server	• Data Domain Replication target
2051	TCP	Replication	• DD Replication Source	• Data Domain Replication target
2052	TCP	DDBoost	• NMC Server	• Data Domain Replication target

The Data Domain system provides functionality to review the network configuration and network capabilities and provides SSH Telnet to help diagnose issues.

Deduplication efficiency

The deduplication ratio measures the efficiency of reduction in storage space that results from the data deduplication and compression technology. Ratios of 20:1 are broadly achievable and reductions of even 5:1 are extremely valuable.

Several factors can contribute to the deduplication ratio:

- Retention periods
- Types of data backed up
- Change rates
- Frequency of full backups
- Use of encryption and compression

For the best use of storage space, consider the factors in the following sections, along with the periodic clearing of expired storage space, and the removal of unused pools.

Retention periods

The deduplication ratio increases with longer data retention periods. The longer you retain the stored save sets, the greater the chance that identical data will exist on the storage that

NetWorker uses to deduplicate each subsequent backup, and the greater is the efficiency of the storage usage.

When you define longer retention periods, the data remains on the Data Domain device for a longer period of time. This enables NetWorker to use the retained data to deduplicate subsequent backups, and results in a more efficient use of storage.

Types of data backed up

Some types of data, for example, text documents, slide presentations, spreadsheets, email, source code, and most database types, contain redundant data and are good deduplication candidates.

Some other types of data, for example, audio, video, and scanned images already consist of compressed data. Typically, the first full deduplication backup of these data types yields low reductions, but subsequent backups generally produce high deduplication ratios if the data has a low change rate.

Change rate

Data with a low change rate changes little between backups, produces high deduplication ratios, and is a good candidate for deduplication. Deduplication removes data that is already in storage and only stores new data.

When a new save set is deduplicated, the number of unique blocks within the save set can vary widely depending on the data type, and often there is little that can be deduplicated. Yet because the Data Domain system compresses the data blocks, there is typically a 2:1 to 3:1 (50%–75%) data reduction.

The storage savings increase with each subsequent backup of the save set because a deduplication backup writes to disk only the data blocks that are unique to the backup. In conventional business operations, the data change rate is typically low and unique data may represent only 1%–2% of the data present in each additional backup set. The remainder of the backup is deduplicated against the data already stored on the system.

Frequency of full backups

Frequent full backups result in high deduplication ratios, but also increase the data processing operations on the NetWorker storage node or Client Direct client. For example, compare daily full deduplication backups with weekly full and added daily incremental deduplication backups. Both of these schedules require essentially the same amount of storage space and the same network bandwidth between the storage node and the Data Domain system. The backups send only unique data to storage, even for full backups.

A daily full backup schedule sends a greater amount of data from the client to the storage node for processing than the weekly full with daily incremental schedule.

Host naming guidelines

The network environment has an impact on hostname resolution methods and you must follow the manufacturer recommendations. Use the local hosts file to help diagnose and resolve naming issues. You can use the `net hosts add` command on the Data Domain system to add hosts to the `/etc/hosts` file.

Use the following guidelines to create consistent, easy-to-identify hostnames that improve the configuration, report generation, and troubleshooting experience in the DD Boost environment:

- Create names that are unique across all NetWorker datazones. Use names that identify the network role, for example, administration, backup, cloning, or production. A name can also include a location or a server name.

- Use a single hostname that is associated with each NIC, IP, or FC interface within the same NetWorker datazone.
- Names can include abbreviations for the source or the target to quickly identify whether the network connections are correct. For example, add an abbreviation of the storage node hostname in the Data Domain name and an abbreviation of the Data Domain hostname in the storage node name. Include the names in the Data Domain `/etc/hosts` file.
- Specify all aliases, such as long and short names and IP addresses, for the NetWorker server and the storage nodes in their respective Client resources. Specify the aliases in the **Aliases** attribute on the **Globals (1 of 2)** tab of a Client resource.
- Test to ensure that you can consistently resolve all hostnames in the network from multiple locations in both directions. For example, ensure that you can resolve the short name to IP address, long name to IP address, IP address to short name, and IP address to long name.
- In general, use short, easy-to-identify, descriptive names instead of IP addresses or fully qualified name strings for devices and storage nodes. Long names may not fit into some views. The following examples include a long name and a short name:
  NWDD365-1.burloak.lab.mycorp.com:/NWDZ_Dr1

  NWDD365-1:/NWDZ_Dr1
- Except for hostnames, use standard alphanumeric characters, including dot (.), hyphen (-), and underscore (_), with no spaces and no special characters. Hostnames may not use underscores (_).
- Use consistent formats, in terms of text field length and text case, and include leading zeros in numbers, with a maximum of 50 characters.
- Avoid the use of dates in names where the dates could change or become meaningless in the future.

Example name formats

The following examples provide some name formats.

DD Boost devices

Format: *Data_Domain_system_name-device_name*

For example: **`dd-tenendo-device01`**

Folders on Data Domain system

Create DD Boost device names that refer to the NetWorker storage node and indicate whether you use them for either backup or clone operations.

Format: *storage_node_name-operation-device_name*

For example: **`dzburl-back-dd01`**

Volume labels for Data Domain

Format: *media_type-label_number*

For example: **`ddmedia-001`**

IP addresses

Avoid IP addresses because numbers are more difficult to identify and troubleshoot than descriptive names. However, there are exceptions:

- The Data Domain system requires the use of IP addresses to interface with an ifgroup for Advanced Load Balancing and Link Failover features.

- For CCRs, the hosts file on the source Data Domain system must list the IP address of the target Data Domain system. Otherwise, the CCR will use the same network access that the backup and restore operations use.

The Data Domain documentation provides details.

Example topologies

This section provides some examples of how you can deploy the Data Domain integration in NetWorker backup environments. Dell EMC recommends that you use two interfaces in Ethernet IP networks, 1 GbE for administration and 10 GbE for data. For FC environments, use IP interfaces for administration and clone operations, and a SAN interface for backup operations. Use the following examples to plan your environment.

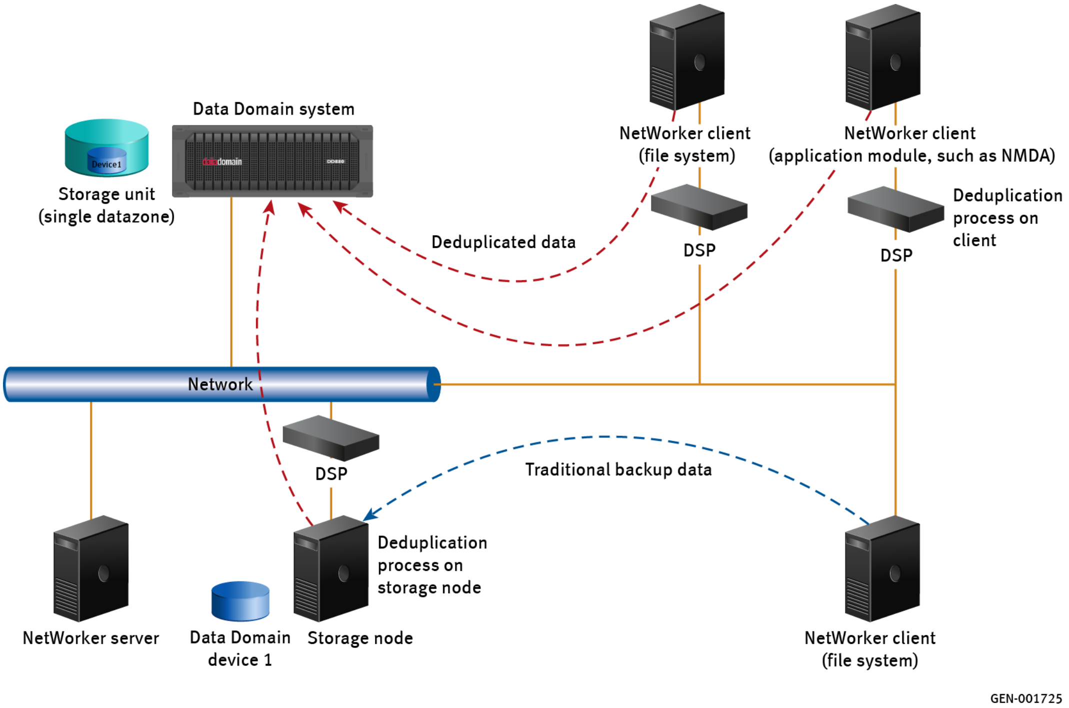
Client Direct deduplication environment

Client Direct functionality is enabled by default in the Client resource and NetWorker tries to use Client Direct for data backup or recovery operations. If the client does not have a direct network connection to the Data Domain system, then these operations automatically use the traditional storage node workflow.

Client Direct data handling on page 17 describes the Client Direct feature, which leverages client DSP software to send deduplicated data directly from a client to a Data Domain system and bypass the storage node.

The following figure shows an example Client Direct environment.

Figure 2 Client Direct backup versus traditional storage node backup



Client Direct deduplication provides the following advantages:

- Deduplication on the client host dramatically reduces the bandwidth that is required for the backup data transfer.

- You can share a single storage volume among multiple DD Boost devices and among multiple backup hosts and storage nodes. You can improve performance and maintainability by configuring multiple hosts and multiple sessions for each device, instead of creating multiple devices.
- Client Direct deduplication offers an alternative to an environment that uses dedicated NetWorker storage nodes, as described in Dedicated storage node environment on page 42. The dedicated storage node environment requires additional licensing and configuration, and the backup clients or the applications on the clients may not support a dedicated storage node.

Disaster recovery environment

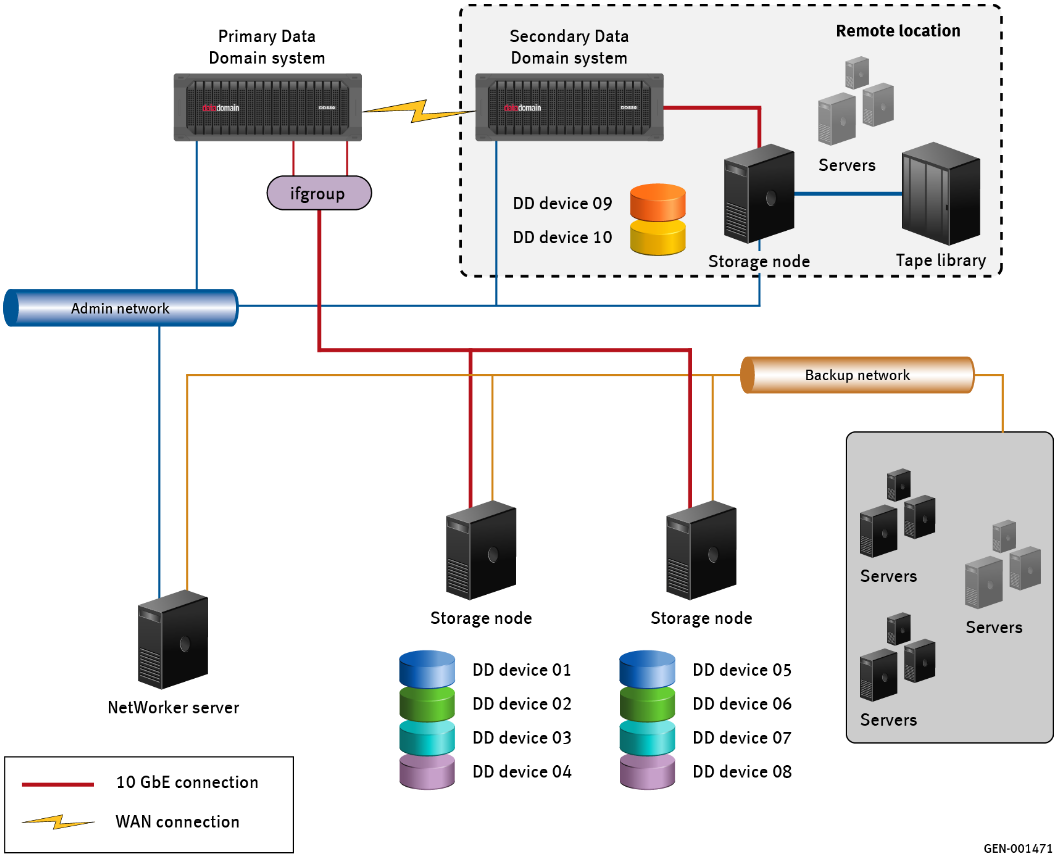
To perform a disaster recovery you can use CCR to copy individual save sets or complete volumes from one Data Domain system to another at a geographically distant location. Each cloned replication, or optimized clone, is a complete and independent copy of the source deduplicated data. NetWorker policies manage both the source or primary data and the clone or secondary data. For additional protection, NetWorker can clone some or all the stored data from the secondary system to tape storage.

You must configure, enable, and manage both the primary and secondary Data Domain systems within a single NetWorker datazone. Configure target devices on the secondary Data Domain system. You can use either a single storage node or separate storage nodes for the local and remote Data Domain system within the datazone.

Note: NetWorker does not support CCR across datazones or to Data Domain devices that are not managed by NetWorker.

The following figure illustrates an example of a disaster recovery environment. The NetWorker server requires two Data Domain Storage System Enablers, one for the primary Data Domain system and one for the remote secondary Data Domain system. DD in the figure signifies Data Domain. The following actions occur in this example:

Figure 3 CCR for disaster recovery



1. The NetWorker server starts the backup of the client groups within the datazone.
2. Two storage nodes in the datazone write the backup data to media pools, which target specific DD Boost devices on the primary system. The pool that is associated with the data protection policy defines which storage devices receive the data.
3. The storage nodes communicate with the primary Data Domain system over a dedicated 10 GbE network connection, and store deduplicated backup data on the devices.

   ⓘ **Note:** An ifgroup configuration of 1 GbE or 10 GbE NICs on the Data Domain system enables multiple storage nodes to use the same network identity. This bandwidth aggregation can improve performance for DD Boost devices. The Data Domain documentation provides details.
4. You can use CCR to store optimized clone copies of backups from the primary Data Domain system over a network to a geographically distant secondary Data Domain system for disaster recovery.
5. An additional option enables a further clone to conventional disk or conventional tape media. A NetWorker storage node, which is attached to the secondary Data Domain system, creates an additional NetWorker clone copy of the data for one of the backup groups, which NetWorker stores on conventional media. NetWorker reverts the data in this copy to the native non-deduplicated format, which is necessary for storage on conventional media.

Cascaded replication environment

A variation of the disaster recovery environment is the cascaded replication environment. Once a deduplicated backup completes successfully, you can use the backup to create multiple clone copies in other locations, either simultaneously from the original deduplicated backup or in sequence from a CCR copy. Each clone replication is a complete and independent copy of the source backup. NetWorker does not limit the number of cascaded clone copies that you can create, provided that the source save set for each clone successfully completes.

As with the previous example, configure, enable, and manage each Data Domain system in a cascaded environment within a single NetWorker datazone. Configure target devices on the Data Domain systems that receive the clone copies.

The figure in this section illustrates an example of a cascaded replication environment with three separate Data Domain systems at three different sites.

- The first site is the primary backup location and is the production site.
- The second site is a local site with good communication links to the production site, typically within the same geographic location as the first site.
- The third site serves as the disaster recovery site, which is located at a geographically distant location. Communication to this more distant site is subject to greater restrictions on bandwidth and latency. This distant site could be in a different country or 250 kilometers (150 miles) or more distant from either of the other two sites.

  ⓘ **Note:** The NetWorker server requires three Data Domain Storage System Enablers, one for each Data Domain system. DR in the figure signifies disaster recovery.

This example environment operates as follows.

1. The NetWorker server starts the backup of production site client groups within its datazone.
2. The production site storage node assigns the backup data to media pools, which uses specific DD Boost devices on the primary Data Domain system.
3. The storage node communicates with the primary Data Domain system over dedicated 10 GbE network connection, and stores deduplicated backup data on devices DD Device 01 and DD Device 02.
4. After the backup completes successfully, you can use CCR to store optimized clone copies of the backups, which reside on the primary Data Domain system, over the network to Data Domain systems at a local secondary site. You can create these clone copies by using one of the following methods:

   - Sequential method—NetWorker performs only one clone operation at a time, in sequence. This method allows the production system to continue to function without the need to create additional clones for a distant site.
     For example, NetWorker uses the original backup on the primary Data Domain system to create an optimized clone copy on a local secondary Data Domain system. Once this process completes, NetWorker uses this copy to create an additional optimized clone copy on the geographically distant Data Domain system.

     Data paths 1a and 1b in the following figure represent this method.

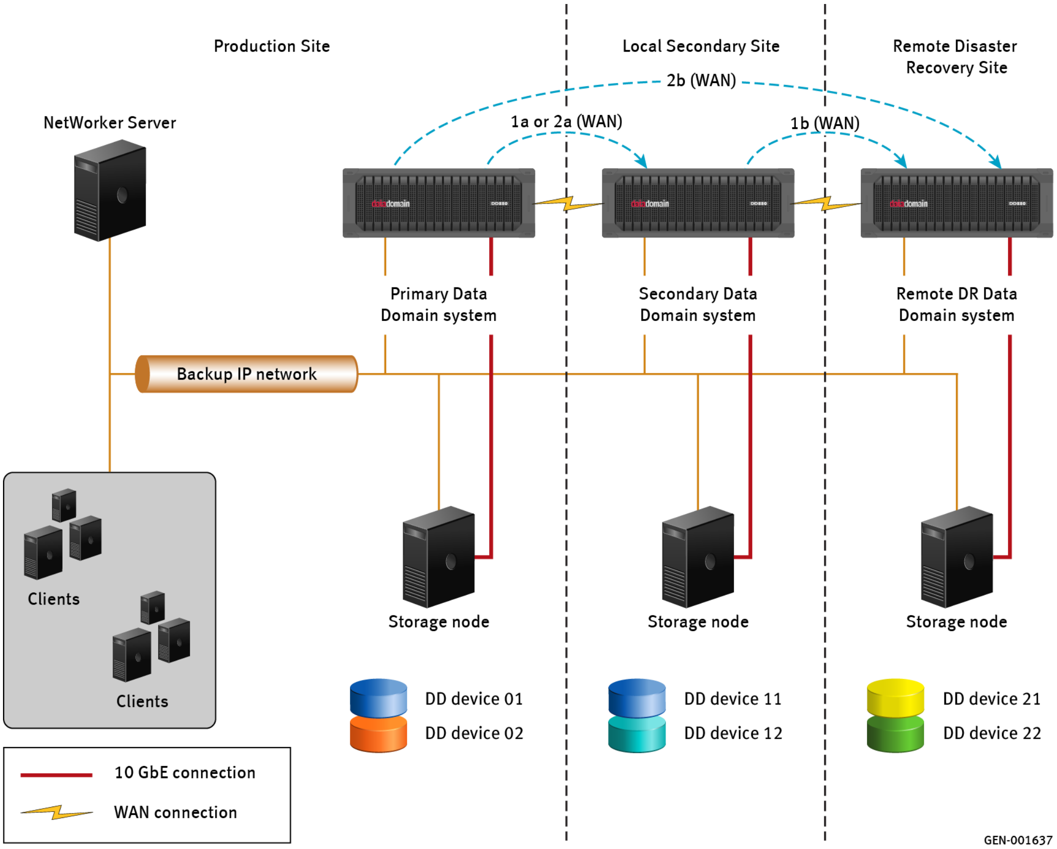
   - Concurrent method—NetWorker may be able to perform the clone operations simultaneously. This method impacts the production system and requires more replication bandwidth.

     ⓘ **Note:** The concurrent method depends on many factors, and you would must validate and test the performance at the individual sites.

     For example, NetWorker uses the original backup on the primary Data Domain system as the source to create simultaneous clones on two target Data Domain systems.

     Data paths 2a and 2b in the following figure represent this method.

Figure 4 CCR cascaded to multiple Data Domain systems



Shared datazones environment

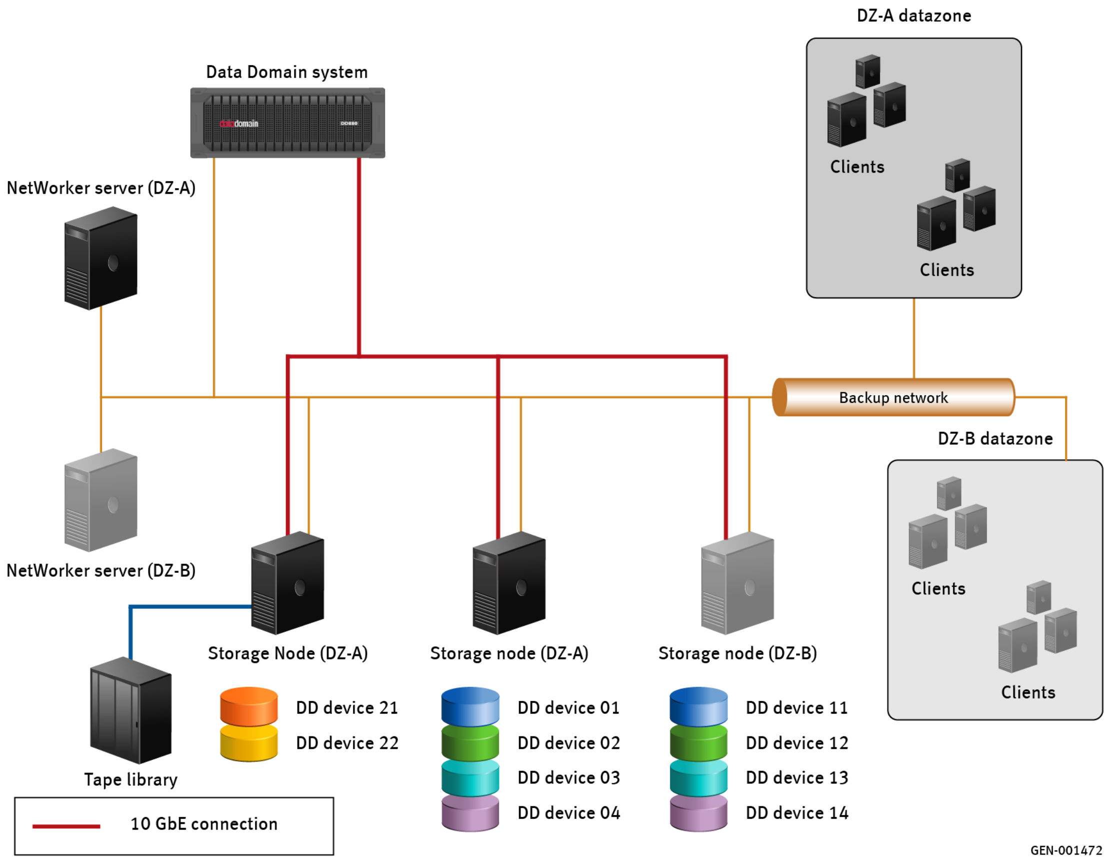
You can store backups from two separate datazones on a single Data Domain system. In this configuration, consider dividing the stream counts and the memory resources to manage the two datazones as separate entities. Do not let one datazone impact the performance of the other datazone. The total number of streams and devices cannot exceed the total capacity of the Data Domain system.

The figure in this section illustrates a dedicated 10 GbE network connection shared by three storage nodes in two NetWorker datazones. Two storage nodes belong to the DZ-A datazone, and one storage node belongs to the DZ-B datazone.

1. The two NetWorker servers begin the backups within their respective datazones.
2. The three storage nodes write the deduplicated backup data to DD Boost storage devices on the Data Domain system over the 10GbE connection. The pool that is associated with the data protection policy defines which storage devices receive the data.

   ⓘ **Note:** You cannot share a DD Boost device across datazones.
3. You can perform an additional backup to tape storage operation, either directly from a storage node or by a NetWorker clone operation from the Data Domain system.

Figure 5 Data Domain system shared across two NetWorker datazones



Dedicated storage node environment

NetWorker supports deduplication backups for high-volume clients that are also a dedicated storage node. For example, you can configure a client host that runs NetWorker Module for Databases and Applications (NMDA) as a dedicated storage node.

This environment can coexist with data protection policy configurations that use shared NetWorker storage nodes in the same datazone. However, because this is a private network, the connection and the devices that the storage node uses are not available to other NetWorker clients.

ⓘ **Note:** The Client Direct (DFA) feature can provide similar benefits without the need for storage node licenses.

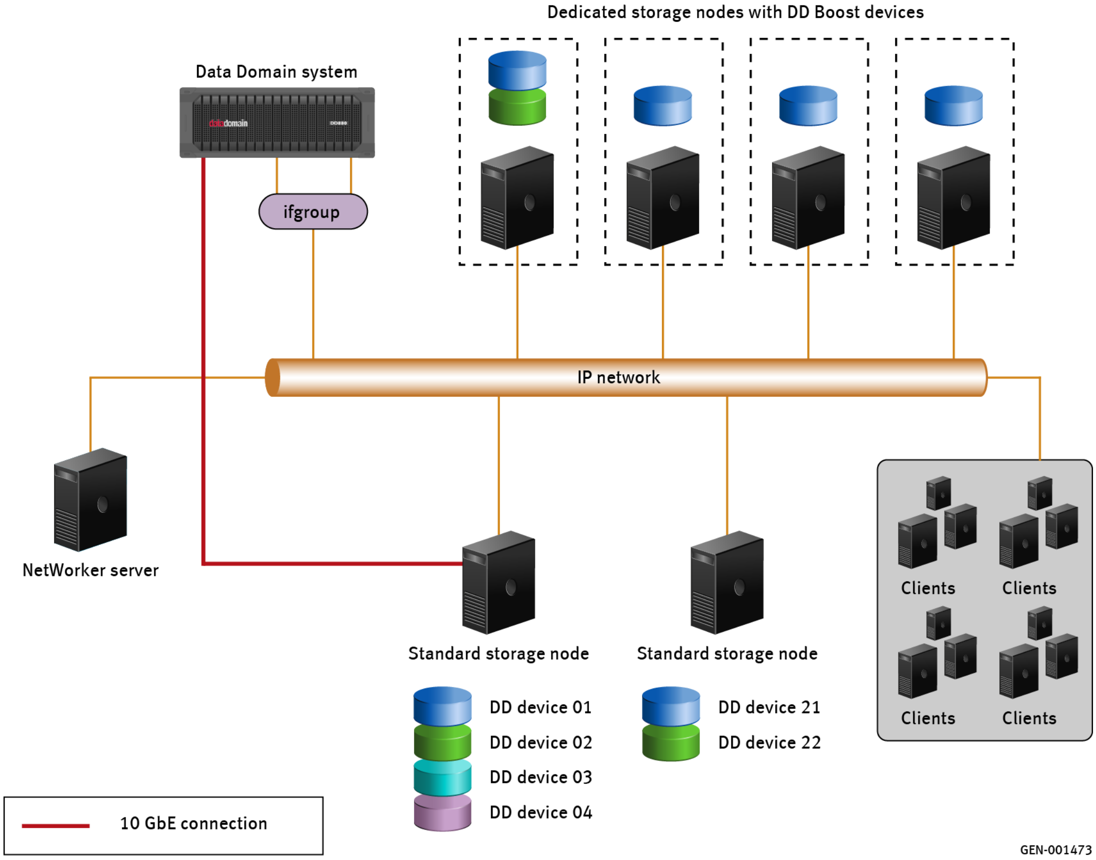
The figure in this section illustrates a mixed environment of shared and dedicated storage nodes.

1. The NetWorker server starts a backup of file system and module data on a dedicated storage node.
2. The storage nodes write the deduplicated backup data to the DD Boost storage devices on the Data Domain system. The pool that is associated with the data protection policy defines which storage devices receive the data.

   ⓘ **Note:** An ifgroup configuration of 1 GbE or 10 GbE NICs on the Data Domain system enables multiple storage nodes to use the same identify on an IP network. This aggregation of bandwidth can improve performance for DD Boost devices. The Data Domain documentation provides details.
3. A high-volume storage node uses an additional dedicated 10 GbE direct connection.

NetWorker E-LAB Navigator provides information on NetWorker application modules compatible with Data Domain systems.

Figure 6 Single datazone with dedicated storage nodes and one high-bandwidth link



CHAPTER 3

Software Configuration

This chapter includes the following topics:

DD Boost and Cloud Tier configuration road map

You can plan the DD Boost and Cloud Tier configurations with a high-level road map that outlines the sequence of basic configuration tasks that you must perform.

1. For DDVE only, configure the DDVE settings.
   Configuring DDVE system settings on page 46
2. Configure the Data Domain system to support DD Boost.
   Configuring the Data Domain system provides details.

   (Optional) For mutli-tenant environments, configure SMT.

   Configuring SMT on the Data Domain system on page 50 provides details.
3. Configure NetWorker devices for use with the Data Domain system by using either Properties window or the Device Configuration Wizard.
   Configuring NetWorker for DD Boost devices provides details.
4. Configure NetWorker devices for the Cloud Tier devices by using the Device Configuration Wizard.
   Configuring NetWorker devices for DD Cloud Tier on page 70 provides details.
5. Configure NetWorker clients to back up to the Data Domain system.
   Configuring clients to back up to DD Boost devices provides details.

Configuring DDVE system settings

After you deploy the Data Domain Virtual Edition (DDVE) appliance and configure the network settings, perform the following steps.

Procedure

1. Log in to the vSphere web client.
2. Right-click the virtual machine and select **Shutdown Guest OS**.
3. Right-click the virtual machine, select **Edit Settings**, and set the configuration options.

   The following settings apply to a DDVE with a 16 TB configuration. Adjust the setting to meet the supported DDVE requirements.

   a. Set the CPU value to a minimum of 4.

   b. Set the Memory value to a minimum of 32 GB.

   c. Add one disk drive with a minimum of 200 GB for the Active Tier.

   d. (Optional) Add one disk drive with a minimum size of 500 GB for the Cloud Tier.

   e. Click **OK**.
4. Right-click the virtual machine and select **Power On**.

Configuring DD Boost on the Data Domain system

Use the Data Domain System Manager or the CLI to configure DD Boost on the Data Domain system.

Configuring the Data Domain system for DD Boost or Cloud Tier by using the Data Domain System Manager

Use the Data Domain System Manager to configure the Data Domain system for DD Boost and Cloud Tier.

Before you begin

Deploy the Data Domain system, create a disk for the storage unit, and complete the network configuration.

Procedure

1. Use a web browser to log in to the **Data Domain System Manager** as the system administrator.
2. In the left navigation pane, select **Hardware** > **Storage**.
3. In the **Active Tier** section, click **Configure**.
4. In the **Addable Storage** table, select the device, which stores backup data, click **Add to Tier**, and then click **Save**.

   ⓘ Note: If a device does not appear in the **Addable Storage** table, add a new disk to the virtual machine.

   The device appears in the **Active Tier** table.
5. (Optional) To configure a Cloud Tier device, perform the following steps:

   a. In the **Cloud Tier** section, click **Configure**.

   b. In the **Addable Storage** table, select the device that stores Cloud data.

   ⓘ Note: If a device does not appear in the **Addable Storage** table, add a new disk to the virtual machine.

   c. Click **Add to Tier**, and then click **Next**.

   The Configure Cloud Tier wizard appears.

   d. Click **Start Assessment**.

   e. Review the Assessment results, and then click **Next**.

   f. Click **Yes**.

   The device appears in the **Cloud Tier** table.
6. In the left navigation pane, select **Data Management** > **File System**, and then click the **Create** button that is located to the left of the file system table.
7. Select the device from the **Active Tier** table and then click **Next**.
8. (Optional) To configure a file system for a Cloud Tier device, perform the following steps:

   a. Select the device from the Cloud Tier table.

   The **Enable Cloud Tier** option appears and the option is enabled.

   b. In the **New Passphrase** and **Confirm Passphrase** fields, specify the passphrase for the Cloud Tier device.

   c. Click **Next**.
9. Review the **Summary** report and click **Next**.

10. Click **Finish**.
11. After the wizard configures the file system and enables the file system feature, click **Close**.
12. a. Add the FQDN of the NetWorker server to the **Allowed Clients** table:
13. In the **Summary** tab, **Protocols** pane, select **NFS export** > **create export**.

    The **Create NFS Exports** window appears.
14. In the **Create NFS Exports** window:

    a. In the **Export Name** field, specify the name of the Data Domain MTree.

    b. In the **Directory path** field, specify the full directory path for Data Domain MTree that you created. Ensure that you use the same name for the directory.

    c. In the **Clients** table, select the NetWorker server, if the NetWorker server does not appear, and then click the **+** (Add) button. In the **Client** field, specify the FQDN of the NetWorker server, and then click **OK**.

Configuring the Data Domain system for DD Boost by using the CLI

You can enable the Data Domain system for storage operations with DD Boost devices by using the Data Domain CLI to complete the following steps.

About this task

The *Data Domain Boost for OpenStorage Administration Guide* provides details.

Procedure

1. Log in to the Data Domain system console as the system administrator user.
2. Use the `license add` command to add the OPENSTORAGE license key, the DD Boost license, and optionally, to enable CCR, the Replication license key:

   ```
   license add license_key
   ```
3. To verify that the file system and the NFS protocol are running, type the following commands:

   ```
   filesys status
   ```

   ```
   nfs status
   ```

   If the services are not running, type the following commands:

   ```
   filesys enable
   nfs enable
   ```

   ⓘ **Note:** For DD Boost functionality, you must enable NFS services on the Data Domain system, even if you do not configure users or shares. You do not need to enable NFS on the NetWorker server, NetWorker storage nodes, or NetWorker clients.
4. To verify the installed version of DD OS, type the following command:

   ```
   system show version
   ```
5. To create one or more new user accounts, type the following command:

   ```
   user add username password password [role role]
   ```

   For example: `user add ddboost password mypassword`
6. To assign the new users as DD Boost users, type the following command:

   ```
   ddboost user assign username-list
   ```

where *username-list* is a comma separated list of usernames.

For example:

```
ddboost user assign bob, joe, sue
```

> **Note:** To unassign one of more users from the DD Boost user list, type the following command:
>
> `ddboost user unassign` ***`username-list`***

7. To restart the Data Domain service and apply the system modifications, type the following commands:

   ```
   ddboost disable
   
   ddboost enable
   ```

8. To configure the system to receive and generate SNMP traps, type the following command.

   ```
   snmp add ro-community community_name
   
   snmp enable
   
   snmp add trap-host hostname[:port]
   ```

   where *community_name* is typically “public”, which allows all users to monitor events.

   SNMP traps enable users to monitor backup events that are captured by SNMP traps.

9. To configure Distributed Segment Processing (DSP), type the following commands:

   a. To enable DSP, type: **`ddboost option set distributed-segment-processing enabled`**

   b. To confirm that DSP is enabled, type: **`ddboost option show`**.

   NetWorker storage nodes and NetWorker clients require DSP to support deduplication operations.

10. (Optional) To enable Fibre Channel (FC) connectivity on DD Boost devices, use the `ddboost fc` command to obtain the DD Boost over FC (DFC) server name:

    ```
    ddboost fc dfc-server-name show
    ```

    > **Note:** You will specify the DFC server name in the NetWorker device configuration procedure. FC-enabled clients can back up only to FC-enabled devices. IP-enabled clients can back up only to IP-enabled devices.

    For example, in the following output, the DFC server name is dd-tenendo:

    ```
    ddboost fc dfc-server-name show
    
    DDBoost dfc-server-name: dd-tenendo
    
    Configure clients to use "DFC-dd-tenendo" for DDBoost FC
    ```

    > **Note:** Do not use the "DFC-" prefix on the DFC server name, as suggested in the output of the `ddboost fc dfc-server-name show` command. This prefix is intended for use with other vendors only and will cause NetWorker communications to the DFC server to fail.

After you finish

To create DD Boost devices and the Data Domain SU folders that contain the devices, use the NetWorker Device Configuration Wizard.

Configuring SMT on the Data Domain system

Enable the Data Domain system for SMT by using the Data Domain CLI to complete the following steps.

About this task

ⓘ **Note:** DDVE does not support SMT.

Procedure

1. Log in to the Data Domain system console with a user account that has the Global Storage Administrator role.
2. Use the `user add` command to create one or more new user account, and assign the *none* role to the user:

   ```
   user add username password password [role role]
   ```

   For example, to create three SMT user accounts named bob, joe and sue, type the following commands:

   ```
   user add bob password mypwbob role none

   user add joe password mypwjoe role none

   user add sue password mypwsue role none
   ```
3. To enable SMT, type the following command:

   ```
   smt enable
   ```
4. To create one or more tenant units (TU), type the following command:

   ```
   smt tenant-unit create tu-name
   ```

   For example, to create a two TUs named tu1 and tu2, type:

   ```
   smt tenant-unit create tu1

   smt tenant-unit create tu2
   ```
5. To assign a default TU to the DD Boost user, type the following command:

   ```
   ddboost user option set username default-tenant-unit tu-name
   ```

   ⓘ **Note:** A DD Boost user can have only one default TU, but multiple DD Boost users can share the same default TU.

   For example, to assign TU tu1 to DD Boost users bob, type:

   ```
   ddboost user option set bob default-tenant-unit tu1
   ```

   To assign TU tu2 to DD Boost users joe and sue, type the following commands:

   ```
   ddboost user option set joe default-tenant-unit tu2

   ddboost user option set sue default-tenant-unit tu2
   ```

Because you assign a default TU to each DD Boost user, NetWorker automatically associates any storage unit (SU) created by a DD Boost user to their default TU. NetWorker does not expose the TUs.

- (Optional) To unassign a DD Boost user from its default TU, or to reassign the user to a different default TU, type the following command:

  ```
  ddboost user option reset username [default-tenant-unit]
  ```

  ⓘ **Note:** Avoid changing the owners of DD Boost SUs. A new owner cannot use the DD Boost devices from a previous owner. Create a device for the new owner instead.

- (Optional) To list the DD Boost users and their default TUs, or the DD Boost users within a specific default TU, type the following command:

  ```
  ddboost user show [default-tenant-unit tenant-unit]
  ```

  ⓘ **Note:** You can use the CLI to review tenant space usage and the performance data at both the TU and SU levels. As the global storage administrator, you can enable tenants to use the Data Domain CLI to review the space usage and the performance data of their TU and SUs. The Data Domain documentation provides details.

Configuring DD Cloud Tier devices

Before you can configure NetWorker to use the DD Cloud Tier devce, you must configure the DD Cloud Tier device on the Data Domain system or DDVE. You cannot use a DD Cloud Tier device as a backup target. A DD Cloud Tier device can only contain a cloned copy of save set data that resides on a DD Active Tier device.

Review the following high-level road map that outlines the sequence of basic configuration tasks that you must perform on the Data Domain system or DDVE:

1. Allocate storage for the DD Cloud Tier device on the Data Domain system.
   Adding DD Cloud Tier storage to a Data Domain System on page 51 provides details.
2. Import the Cloud Service Provider certificate.
   Import the cloud certificate on page 52 provides details.
3. Create the cloud profile and cloud unit.
   Create the cloud profile and the cloud unit on page 53 provides details.

Adding DD Cloud Tier storage to a Data Domain System

Use the DD System Manager or the CLI to add a DD Cloud Tier storage to an existing Data Domain system. You must configure the DD Cloud Tier storage on the same Data Domain storage unit as the DD Active Tier.

Adding a DD Cloud Tier storage to the Data Domain system by using the CLI

Before you begin

On a DDVE, add new storage to the virtual machine for the Cloud Tier.

Procedure

1. Log in to the Data Domain system console as the sysadmin user.
2. To enable the Cloud Tier feature, type the following command:

   ```
   cloud enable
   ```

3. At the **Do you want to enable encryption?** prompt, type `Yes`.

4. At the **New Passphrase** prompt, type a passphrase for Cloud Tier encryption.
5. At the **Confirm Passphrase** prompt, type a passphrase for Cloud Tier encryption.
6. To configure the Cloud Tier device, type one of the following commands:
   - Data Domain system—`storage add tier cloud enclosures` ***`number`***
     where *number* is the device number.
   - DDVE—`storage add tier cloud` ***`device`***
     where *device* is the name of the device, for example `dev4`.

Adding a DD Cloud Tier by using Data Domain System Manager

Perform the following steps to add DD Cloud Tier storage to an existing Data Domain system.

Before you begin

The DD Cloud Tier feature requires a Cloud Tier Capacity license.

Procedure

1. Use a web browser to log in to the **Data Domain System Manager** as the system administrator.
2. In the left navigation pane, select **Hardware** > **Storage**.
3. Click **Configure**, located above the **Cloud Tier** table.
4. From the **Addable Tier** table:

   a. Select an available disk.

   b. Click **Add to Tier**.

   c. Click **Next**.

   > Note: If a device does not appear in the **Addable Storage** table, add a new disk to the virtual machine.

   The **Configure Cloud Tier** wizard appears.
5. Click **Start Assessment**.
6. Review the assessment results, and then click **Next**.
7. Click **Yes**.

   The device appears in the **Cloud Tier** table.

Import the cloud certificate

Obtain the cloud certificate from the Cloud Service Provider and use DD System Manager or the CLI to import the certificate on the Data Domain system or DDVE.

Importing cloud certificates by using the CLI

Perform the following steps to import the cloud certificate onto the Data Domain system or DDVE.

Procedure

1. On a host that has network access to the Data Domain System or DDVE download the PEM certificate files from the Cloud Service Provider.
2. Copy the PEM files to the certificates directory on the Data Domain System or DDVE.

   For example, use the SCP application or ftp. The certificates directory is located in `/ddvar/certificates (DDVE).`

3. Log in to the Data Domain console as the sysadmin user.
4. Import the certificate by typing the following command:

   ```
   adminaccess certificate import ca application cloud file pem_file_name
   ```

Importing cloud certificates by using the DD System Manager

Perform the following steps to import the cloud certificate onto the Data Domain system or DDVE.

About this task

Perform the following steps from a host that had network access to the Data Domain system or DDVE.

Procedure

1. Download the PEM certificate files from the Cloud Service Provider.
2. On the host that contains the PEM files, use a web browser to log in to the DD System Manager with the sysadmin user account.
3. On the left navigation pane, select **Data Management** > **File System**.
4. On the **Cloud Units** tab, click **Manage Certificates**, and then click **Add**.
5. On the **Add CA Certificate for Cloud** window, click **Choose File**, select the CA PEM file, and then click **Open**.
6. Click **Add**.
7. Click **OK**.
8. Click **Close**.

Create the cloud profile and the cloud unit

Create the cloud profile and the cloud unit on the Data Domain system or DDVE by using the CLI or the DD System Manager.

Creating the Cloud Profile and Cloud Unit by using the CLI

Data Domain supports a maximum of two Cloud Units.

About this task

Perform the following steps on the Data Domain system or DDVE to create the Cloud Profile and Cloud Unit.

Procedure

1. Log in to the Data Domain system or DDVE as the sysadmin user.
2. Type the following command to create the Cloud Profile:

   ```
   cloud profile add profile_name
   ```
   where *profile_name* is a descriptive name for the profile.

3. At the **Enter provider name** prompt, type the name of the provider:
   - Dell EMC Elastic Cloud Storage (ECS)—ecs
   - Virtustream Cloud Storage—virtustream
   - Amazon Web Services S3—aws
4. For the Virtustream Storage Cloud provider only, at the **Enter Storage Class** prompt, type the storage class.

5. For the Virtustream Storage Cloud and Amazon Web Service S3 providers only, at the **Enter Storage Region** prompt, type the storage region.
6. At the **Enter the access key** prompt, type the cloud provider access key.
7. At the **Enter the secret key** prompt, type the cloud provider secret key.
8. For Dell EMC Elastic Cloud Storage (ECS) only, at the **Enter the endpoint** prompt, type the load balancer endpoint address for the cloud provider.

   For example: `http://172.21.21.10:9020`

   Load balancer is mandatory for all ECS Cloud Tier deployments.
9. At the **Do you want to enter proxy details** prompt, press **Enter** to accept the default value, no.
10. Type the following command to add a new Cloud Unit:

    ```
    cloud unit add unit_name profile profile_name
    ```
    where:

    - *unit_name* is a descriptive name for the Cloud Unit, for example `cloud-unit-1`.
    - *profile_name* is the name of the cloud profile that you created.

    For example:

    ```
    sysadmin@localhost#cloud unit add cloud-unit-1 profile ecs_profile
    Cloud unit 'cloud-unit-1'created successfully.
    ```

Creating the Cloud Profile and Cloud Unit by using Data Domain System Manager

Data Domain supports a maximum of 2 Cloud Units.

About this task

Perform the following steps to create the Cloud Profile and Cloud Unit.

Procedure

1. Use a web browser to log in to the **Data Domain System Manager** as the system administrator.
2. In the left navigation pane, select **Data Management** > **File System**.
3. On the **Cloud Units** tab, click **Add**.
4. In the **Name** field, provide a descriptive name for the Cloud Unit.
5. In the **Cloud Provider** list, select the cloud provider.
6. For the Virtustream Storage Cloud provider only, in the **Storage Class** field, type the storage class.
7. For the Virtustream Storage Cloud and Amazon Web Service S3 providers only, in the **Storage Region** field, type the storage region.
8. In the **Access key** field, specify the cloud provider access key.
9. In the **Secret key** field, specify the cloud provider secret key.
10. For Dell EMC Elastic Cloud Storage (ECS) only, in the Endpoint field, specify the load balancer endpoint address for the cloud provider.
11. Click **OK**.

Results

The **Cloud Units** page displays information about the Cloud Unit, and the status of the unit is **Enabled**.

Create the data movement schedule

The data movement schedule determines the frequency in which data moves from the DD Cloud Tier device to the cloud provider.

Before you configure the data movement operation to the cloud for long term storage, consider the day of the week, time of day, and frequency in which you will schedule the movement operation. The data movement command moves all data that is available on the DD Cloud Tier device to the Cloud provider. Ensure that you define a frequency that allows you to move the data over a period of time that does not impact your network. Define a day of the week and time when network bandwidth and the cost of moving the data is low.

Create the data movement schedule on the Data Domain system or DDVE by using the CLI or the Data Domain System Manager.

Creating a data movement schedule by using the CLI

Use the `data-movement` command to create a schedule for data movement from the DD Cloud Tier device to the cloud provider.

Procedure

1. Log in to the Data Domain system or DDVE as the sysadmin user.
2. To create the data movement schedule, type:

   data-movement schedule set to-tier cloud days "*day_of_week*" time "*hh:mm*" [every *n* wks]

   where:

   - *day_of_week* is the day of the week in which to run the data movement operation. For example, Thursday.
   - *hh:mm* is the time in hours and minutes in which to run the data movement operation. For example, to start the data movement operation at 11 pm, type **23:00**.
   - [every *n* wks] is option and defines the frequency in which to run the data movement operation. For example, to run the data movement operation bi-monthly, type **every 2 weeks**. If you do not use this option, the data movement operation runs weekly.

   For example, to schedule the data movement operation to run every two weeks at 11 pm on a Thursday, type:

   ```
   data-movement schedule set to-tier cloud days "Thursday" time "23:00"
   every 2 wks
   ```

   Output similar to the following appears:

   ```
   Data-movement schedule has been set.
   Data-movement is scheduled to run on day(s) "thu" at "23:00" hrs
   every "2" week(s).
   ```
3. To display the data movement schedule, type

   ```
   data-movement schedule show
   ```

   Output similar to the following appears:

```
Data-movement is scheduled to run on day(s) "thu" at "23:00" hrs
every "2" week(s).
```

Creating a data movement schedule by using Data Domain System Manager

Perform the following steps to create a data movement schedule on the Data Domain system or DDVE.

About this task

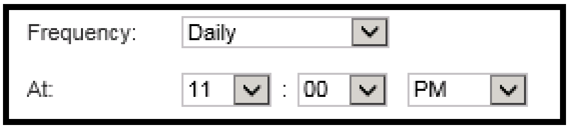
Perform the following steps from a host that had network access to the Data Domain system or DDVE.

Procedure

1. Use a web browser to log in to the **Data Domain System Manager** as the system administrator.
2. In left navigation pane, select **Data Management** > **File System**.
3. Click **Settings**, and then select the **Data Movement** tab.
4. In the **Throttle** section, leave the default value of 100%.

   The *Data Domain Operating System Command Reference Guide* provides more information about data movement throttling.
5. In the **Schedule** section, from the **Frequency** list, select one of the following options:
   - Daily—From each **At** box, select the hour, minute, and **AM** or **PM**. The following figure provides an en example of a schedule that runs daily at 11 P.M.

     Figure 7 Daily data movement schedule

     Frequency: Daily
     At: 11 : 00 PM

   - Weekly—Configure the schedule by performing the following steps:

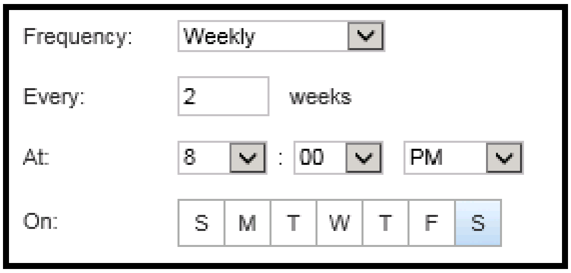
     a. In the **Every** field, type the number of weeks in which to run the schedule. For example, to run the movement operation bi-monthly, type 2.

     b. From each **At** box, select the hour, minute, and **AM** or **PM**.

     c. In the **On** field, select the day of the week in which to run the schedule.

     The following figure provides an example of a bi-monthly movement schedule that occurs every Saturday at 8 P.M.

     Figure 8 Weekly data movement schedule

     Frequency: Weekly
     Every: 2 weeks
     At: 8 : 00 PM
     On: S M T W T F S

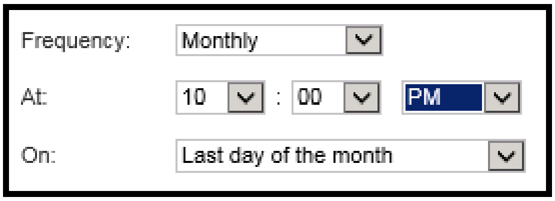
   - Monthly—From each **At** box, select the hour, minute, and **AM** or **PM**. In the **On** field, perform one of the following steps:

a. To schedule the movement to occur on a specific date in the month, leave the default selection **Dates**, and then select the day of the month on which to schedule the movement.

b. To schedule the movement to occur on the last day of every month, select **Last Day of the Month**.

The following figure provides an example of a movement schedule that occurs on the last day of each month.

Figure 9 Monthly data movement schedule



Frequency: Monthly

At: 10 : 00 PM

On: Last day of the month

6. Click **OK**.

Configuring a Highly Available Data Domain system

NetWorker 19.2 supports highly available Data Domain systems.

About this task

When a highly available Data Domain system fails over to its standby node, NMC generates an HA Setup Degraded event. If there is an ambiguity in time between the Active Node and the Standby Node, NMC generates the HA Setup Out-of-Sync event.

All in-progress NetWorker operations including backup, clone, and recover operations are unaffected, except for a temporary freeze of operations for a few minutes. However, during unusually long freezes of ten minutes or more, some NetWorker operations might fail and are automatically retried. Some failed NetWorker operations might require a manual restart.

If interrupted by a failover the following processes fail, NFS, VTL, and CIFS jobs. To restart or resume NFS, VTL, and CIFS failed jobs, you must configure NetWorker policies to restart the failed jobs. Restart the failed jobs as soon as the failover completes, however you must manually restart the jobs. The failed jobs will not restart or resume on their own.

ⓘ Note: To view events in NMC, clear all alerts on the Data Domain system. For example, in the Data Domain UI, select **Alerts** > **Current Alerts** > **Select All** > **Clear**.

For each node in the cluster, perform the following tasks.

Procedure

1. Log in to the NMC GUI as an administrator of the NetWorker server.
2. On the taskbar, click the **Enterprise** icon .
3. In the left navigation pane:

   a. Right-click **Enterprise**.

   b. Select **New** > **Host**.

   The **Add New Host** wizard appears.
4. In the **Create Host** page:

   a. Depending on the node in the cluster, specify the following:

- For the highly available Data Domain system, specify the floating IP.
- For node 1, specify the hostname with the correct community string.
- For node 2, specify the hostname with the correct community string.

b. Click **Next**.

5. In the **Select Host Type** page:

   a. Select **DataDomain**.

   b. Click **Next**.

6. In the **Manage DataDomain** page:

   a. Review the configuration details.

   b. Click **Next**.

   c. Leave the **Capture Events** option selected.

7. (Optional) In the **Configure SNMP Monitoring** page, perform the following steps:

   a. In the **SNMP Community String** field, type the name of the SNMP community string.

   ⓘ **Note:** If you do not know the name of the community, leave this field blank.

   b. With the **Receive SNMP trap events** option selected, specify the **SNMP Process** port that is used by the Data Domain system and select the events in which to monitor. Use the **Reset to defaults option** to reset the events in which to monitor back to the default settings.

   ⓘ **Note:** The default SNMP process port is 162.

   c. Click **Next**.

   SNMP monitoring enables NMC to display the Data Domain system status and to list the backup and the recovery events. The monitoring feature also provides a launcher link for the Data Domain interface.

   d. Click **Finish**.

8. Configure alerts for Data Domain High Availability events:

   a. Click the Devices button on the taskbar.

   b. In the left navigation pane, right-click **Data Domain Systems** and select **New Device Wizard**.

   c. Open the SNMP Monitoring Options page and select the following options:

   - HA Setup Degraded
   - HA Setup Offline
   - HA Setup Out-of-Sync

Configuring NetWorker for DD Boost devices

After you configure a Data Domain system for the DD Boost environment, you can configure the NetWorker resources for devices, media pools, volume labels, clients, and groups that use the DD Boost devices.

Keep the following NetWorker considerations in mind:

- Each DD Boost device appears as a folder on the Data Domain system. A unique NetWorker volume label identifies each device and associates the device with a pool.
- NetWorker uses pools to direct backups or clones of backups to specific local or remote devices.
- NetWorker uses Data Protection policy resources to specify the backup and cloning schedules for member clients. It is recommended that you create policies that are dedicated solely to DD Boost backups.
- VMware Backup Appliance does not support the SMT feature. The *NetWorker VMware Integration Guide* provides details.

DD Boost device performance considerations

NetWorker does not limit the number of DD Boost devices that you can create. The number of required devices depends on device usage for backup operations and restore operations.

Increasing the number of DD Boost devices can impact Data Domain performance and maintenance. Typically, if you do not need multiple concurrent sessions or streams for recovery, then you can configure the device Target Sessions and Max Sessions settings for multiple concurrent backup sessions. Avoid the removal of DD Boost devices.

Configuring DD Boost devices with the NMC Device Configuration wizard

Use the NMC NetWorker Administration Device Configuration wizard to create or modify Data Domain devices, and to define the Data Domain system on the NetWorker server.

Procedure

1. Log in to the NMC GUI as an administrator of the NetWorker server.
2. On the taskbar, click the **Enterprise** icon .
3. In the navigation tree, highlight a host:

   a. Right-click **NetWorker**.

   b. Select **Launch Application**. The **NetWorker Administration** window appears.
4. On the taskbar, click the **Devices** button .
5. In the left navigation pane:

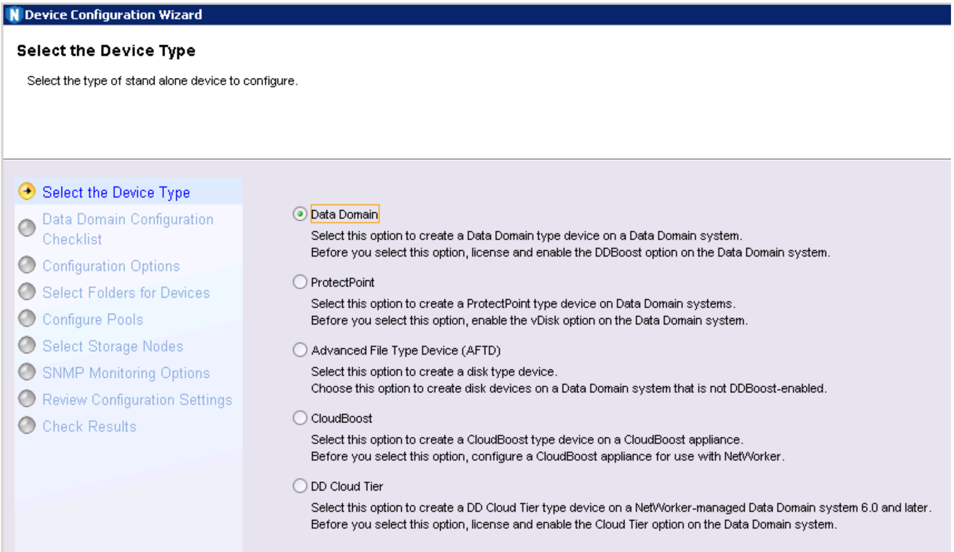
   a. Right-click **Data Domain Systems**.

   b. Select **New Device Wizard**.

   ⓘ **Note:** To modify completed wizard pages, click the links in the steps panel. The number of steps may vary according to the type of configuration chosen.
6. In the **Select the Device Type** page, select the **Data Domain** device type, and then click **Next**.

   The following figure provides an example of the **Select the Device Type** page.

Figure 10 Select the Device Type page



Device Configuration Wizard

Select the Device Type

Select the type of stand alone device to configure.

- Select the Device Type
- Data Domain Configuration Checklist
- Configuration Options
- Select Folders for Devices
- Configure Pools
- Select Storage Nodes
- SNMP Monitoring Options
- Review Configuration Settings
- Check Results

● Data Domain

Select this option to create a Data Domain type device on a Data Domain system.
Before you select this option, license and enable the DDBoost option on the Data Domain system.

○ ProtectPoint

Select this option to create a ProtectPoint type device on Data Domain systems.
Before you select this option, enable the vDisk option on the Data Domain system.

○ Advanced File Type Device (AFTD)

Select this option to create a disk type device.
Choose this option to create disk devices on a Data Domain system that is not DDBoost-enabled.

○ CloudBoost

Select this option to create a CloudBoost type device on a CloudBoost appliance.
Before you select this option, configure a CloudBoost appliance for use with NetWorker.

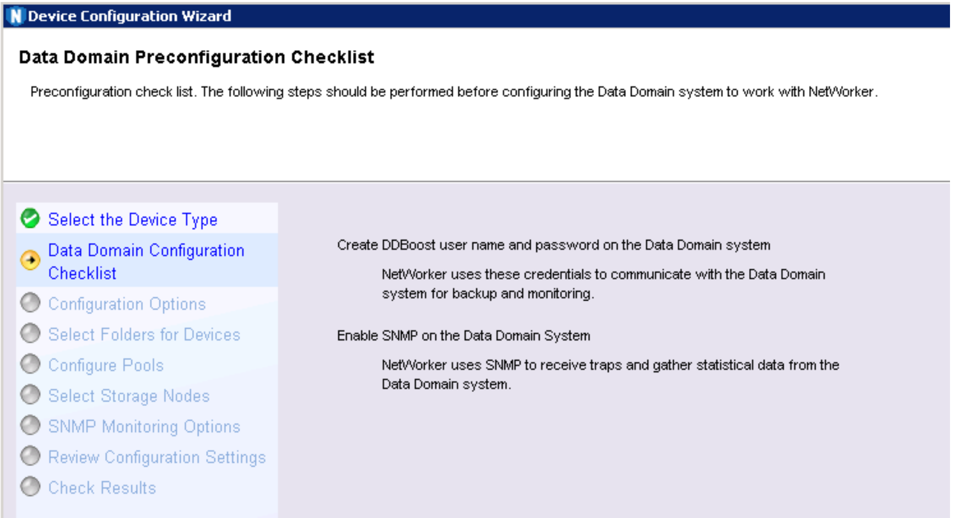
○ DD Cloud Tier

Select this option to create a DD Cloud Tier type device on a NetWorker-managed Data Domain system 6.0 and later.
Before you select this option, license and enable the Cloud Tier option on the Data Domain system.

7. In the **Data Domain Preconfiguration Checklist** page, review the requirements, and then click **Next.**

   The following figure provides an example of the **Data Domain Preconfiguration Checklist** page.

Figure 11 Data Domain Preconfiguration Checklist page



Device Configuration Wizard

Data Domain Preconfiguration Checklist

Preconfiguration check list. The following steps should be performed before configuring the Data Domain system to work with NetWorker.

- ✓ Select the Device Type
- Data Domain Configuration Checklist
- Configuration Options
- Select Folders for Devices
- Configure Pools
- Select Storage Nodes
- SNMP Monitoring Options
- Review Configuration Settings
- Check Results

Create DDBoost user name and password on the Data Domain system

NetWorker uses these credentials to communicate with the Data Domain system for backup and monitoring.

Enable SNMP on the Data Domain System

NetWorker uses SNMP to receive traps and gather statistical data from the Data Domain system.

8. In the **Specify the Data Domain Configuration Options** page, configure the following fields:

   a. In the **Data Domain System** section, select one of the following options:

   - To use a Data Domain system on which you have previously created devices or configured as a managed host, select **Use an existing Data Domain System**, and then select the host.
   - To use a new Data Domain system, select **Add a new Data Domain System**, and then type the FQDN or IP address of the Data Domain system or DDVE.

   > Note: If you use DFC connectivity, Do not use the "DFC-" prefix on the DFC server name, as suggested in the output of the `ddboost fc dfc-server-name show`

command. This prefix is intended for use with other vendors only and will cause NetWorker communications to the DFC server to fail.

b. In the **DD Boost Credentials** section, type the username for the DD Boost user in the **DD Boost Username** field.

c. In the **Secure Multi-Tenancy** section, to use only DD Boost devices in secure Storage Units (SUs), select **Configure Secure Multi-Tenancy (SMT)**, and then perform one of the following tasks:

- To use an existing storage unit (SU), select **Use an existing secure storage unit**, and then select the SU.
- To create a SU, select **Create a new secure storage unit**, and then specify the name of the SU.

ⓘ Note: SMT restricts access of each SU to one owner according to the provided DD Boost credentials.

d. (Optional) In the **DD Management Credentials** section, configure the management credentials that are required to perform VMware Instant Access and FLR recoveries:

- To not specify the management credentials, leave the default selection **Don't configure Management Credentials now**.
- To instruct NetWorker to use the DD Boost user credentials that you specified in the **DD Boost Credentials** section, select **Use the DDBoost Credentials from above**.
- To specify a different sysadmin user, select **Enter Management Credentials**, and then specify the username and password of a sysadmin user.

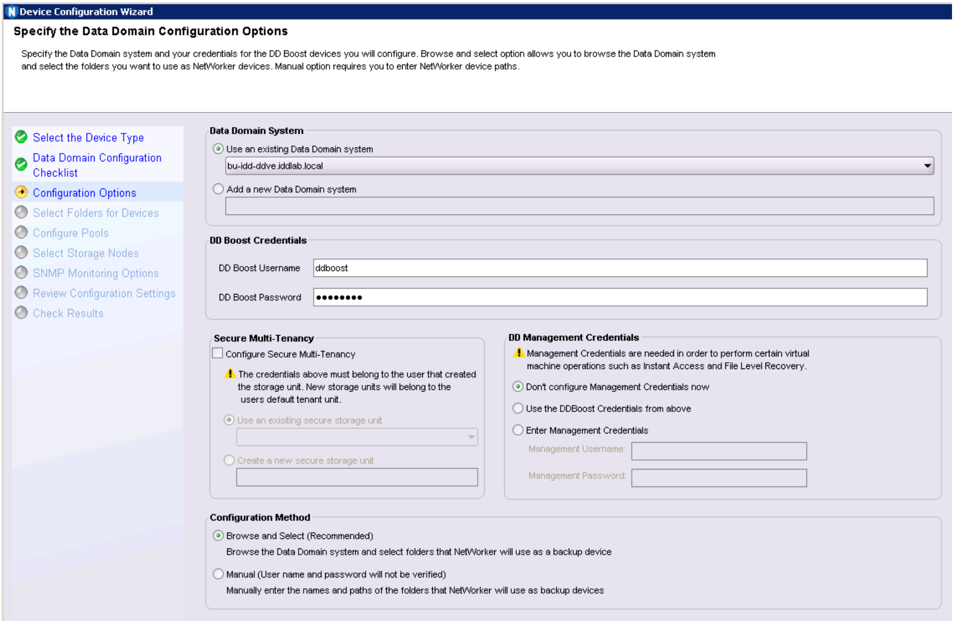
ⓘ Note: If you plan to use the REST API for features such as DD Cloud Tier policy creation and DD Retention Lock, you must additionally update the **NSR Data Domain** RAP resource with the Management username, password, port, and host. If these credentials and details are not specified in the RAP resource, then a validation error occurs.

e. In the **Configuration Method** field, select **Browse and Select**, and then click **Next**.

ⓘ Note: If you do not configure the SMT option, the wizard will create an SU for you on the Data Domain system, and name the SU after the shortname of the NetWorker server.

The following figure provides an example of the **Specify the Data Domain Configuration Options** page.

Figure 12 Specify the Data Domain Configuration Options page



Device Configuration Wizard

Specify the Data Domain Configuration Options

Specify the Data Domain system and your credentials for the DD Boost devices you will configure. Browse and select option allows you to browse the Data Domain system and select the folders you want to use as NetWorker devices. Manual option requires you to enter NetWorker device paths.

- ✓ Select the Device Type
- ✓ Data Domain Configuration Checklist
- ➔ Configuration Options
- Select Folders for Devices
- Configure Pools
- Select Storage Nodes
- SNMP Monitoring Options
- Review Configuration Settings
- Check Results

Data Domain System

● Use an existing Data Domain system: bu-idd-ddve.iddlab.local

○ Add a new Data Domain system

DD Boost Credentials

DD Boost Username: ddboost

DD Boost Password: ••••••••

Secure Multi-Tenancy

□ Configure Secure Multi-Tenancy

⚠ The credentials above must belong to the user that created the storage unit. New storage units will belong to the users default tenant unit.

● Use an exisiting secure storage unit

○ Create a new secure storage unit

DD Management Credentials

⚠ Management Credentials are needed in order to perform certain virtual machine operations such as Instant Access and File Level Recovery.

● Don't configure Management Credentials now

○ Use the DDBoost Credentials from above

○ Enter Management Credentials

Management Username:

Management Password:

Configuration Method

● Browse and Select (Recommended)
Browse the Data Domain system and select folders that NetWorker will use as a backup device

○ Manual (User name and password will not be verified)
Manually enter the names and paths of the folders that NetWorker will use as backup devices

9. In the **Select Folders to use as Devices** page, to create a DD Boost device, perform the following steps:

   a. Select the Data Domain system, and then click **New Folder**.

   A new folder appears in the navigation tree. This folder is the new device.

   Note: The navigation tree does not show the SU folder under the Data Domain system folder. However, the SU folder is verifiable in the final **Review Configurations Settings** wizard page. The wizard names the SU folder after the short hostname of the NetWorker server and places the devices that you create into this SU folder.

   b. Type a name for the new folder, and then select the checkbox next to the folder or device name.

   The Device table displays the full NetWorker device name, the storage pathname, and details about the device.

   Note: The device name refers to the subfolder created within the SU. The folder path must not contain other folders deeper than these device folders.

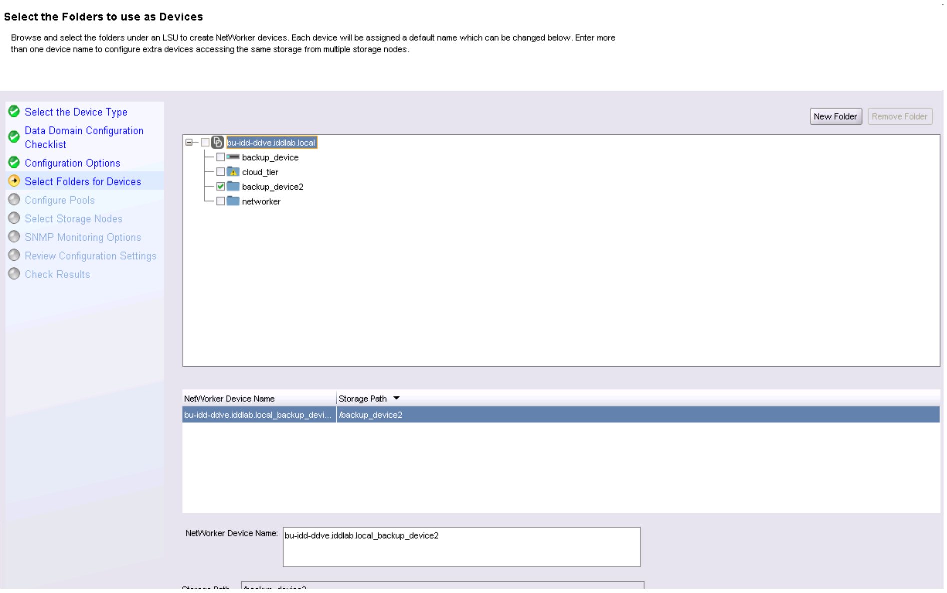
   c. (Optional) To rename a DD Boost device as it appears in NMC, select the device in the table, and type a new name in the **NetWorker Device Name** field. Do not use special characters other than dot (.) and underscore (_). The **Storage Path** field remains unchanged.

   Note: Implicit in the SU folder pathname on the Data Domain system is the hidden mount point folders `/data/col1`. Do not modify this folder structure, which all NetWorker server hosts use. The final wizard page, **Review Configurations Settings**, shows the complete location.
   The `/backup` folder stores NFS service data. The clients that are configured for NFS access can view, change, and delete the `/data/col1` directory that contains the DD Boost devices. If you use NFS devices, you can avoid the risk of potential interference by using alternative path names.

d. Click **Next**.

The following figure provides an example of the **Select the Folders to use as Devices** page.

Figure 13 Select the Folders to use as Devices page



Select the Folders to use as Devices

Browse and select the folders under an LSU to create NetWorker devices. Each device will be assigned a default name which can be changed below. Enter more than one device name to configure extra devices accessing the same storage from multiple storage nodes.

NetWorker Device Name	Storage Path
bu-idd-ddve.iddlab.local_backup_devi...	/backup_device2

NetWorker Device Name: bu-idd-ddve.iddlab.local_backup_device2

10. On the **Configure Pool Information** page, perform the following steps:

    a. Select **Configure Media Pools for Devices**.

    b. In the **Pool Type** section, select the type of data to send to the Data Domain device, either **Backup** for backups or **Backup Clone** for cloning or staging operation.

    c. In the **Pool** section, select **Create and use a new Pool** to create a pool to receive the data, or select **Use an existing Pool** to select a pool that exists on NetWorker server.

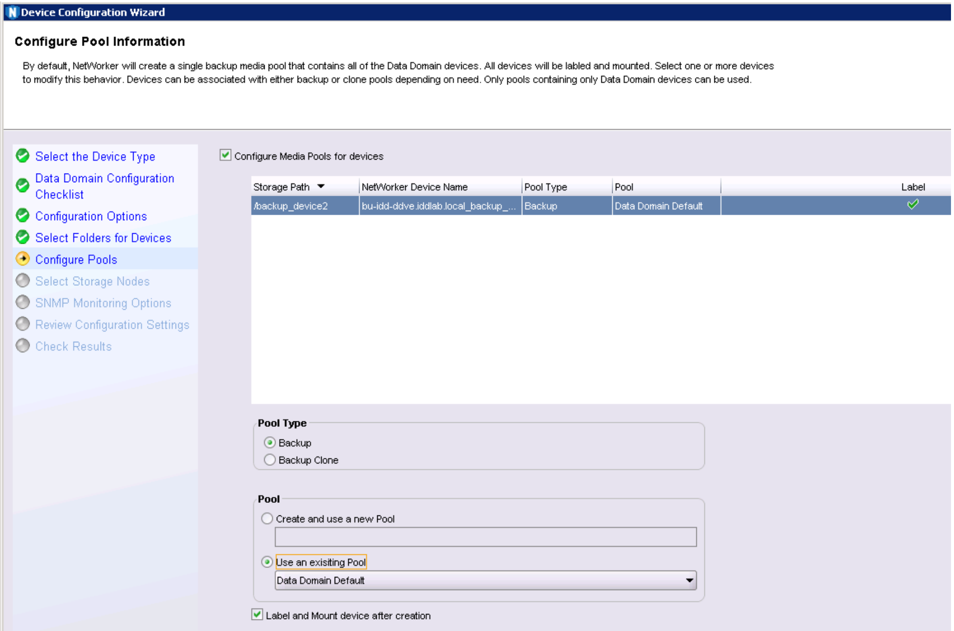
    NetWorker provides a preconfigured Data Domain pool that you can select, named Data Domain Default.

    d. Leave the **Label and Mount device after creation** option selected.

    e. Click **Next**.

    The following figure provides as example of the **Configure Pool Information** page.

Figure 14 Configure Pool Information page



Device Configuration Wizard

Configure Pool Information

By default, NetWorker will create a single backup media pool that contains all of the Data Domain devices. All devices will be labled and mounted. Select one or more devices to modify this behavior. Devices can be associated with either backup or clone pools depending on need. Only pools containing only Data Domain devices can be used.

- Select the Device Type
- Data Domain Configuration Checklist
- Configuration Options
- Select Folders for Devices
- Configure Pools
- Select Storage Nodes
- SNMP Monitoring Options
- Review Configuration Settings
- Check Results

☑ Configure Media Pools for devices

Storage Path	NetWorker Device Name	Pool Type	Pool	Label
/backup_device2	bu-idd-ddve.iddlab.local_backup_...	Backup	Data Domain Default	✓

Pool Type
● Backup
○ Backup Clone

Pool
○ Create and use a new Pool
● Use an existing Pool: Data Domain Default

☑ Label and Mount device after creation

11. On the **Select Storage Nodes** page, perform the following steps:

   a. In the **Storage Node Options** section, specify the storage node that manages the device.

   - To use an existing storage node on the NetWorker server, select **Use an existing storage node**.
   - To use a new storage node, select **Create a new storage node**, and then type the hostname of a storage node host.
     If the new Storage Node is also a Dedicated Storage Node, select **Dedicated Storage Node**.

   b. (Optional) To enable FC data transport for this device, perform the following steps:

   - Select **Enable Fibre Channel**.
   - In the **Fibre Channel Host Name** field, type the hostname that the Data Domain system uses to identify itself for FC operations. By default, this hostname is the same name used for IP operations, but the hostnames can be different. The hostname must match the Server Name displayed on the Data Domain system in the **Data Management** > **DD Boost** > **Fibre Channel** tab of the **Data Domain Enterprise Manager**. The name is case-sensitive.

     Note: All NetWorker clients that use an FC-enabled DD Boost device must be enabled for FC in the **Data Domain Interface** field.

   c. Enable or disable DD Retention Lock on the device:

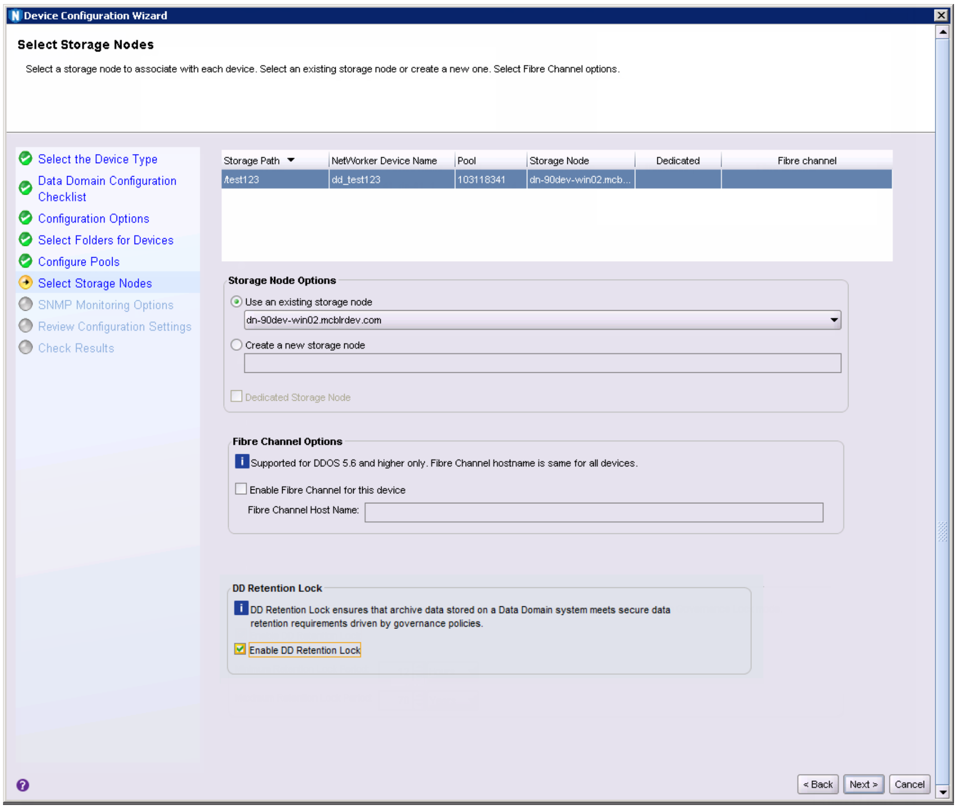
   - Select **Enable DD Retention Lock** to enable this feature, and click **Next**. If you do not have the minimum DDOS version required to use DD Retention lock, an error appears requesting you to install version 6.0 or later. Currently, support for DD Retention lock is applicable to **Governance** Lock mode and **Compliance** Lock mode.

     Note: You must also select **Apply DD Retention Lock** in the **Policy action** wizard so that DD Retention lock gets applied to save sets in the NetWorker data protection policy.
   - Unselect **Enable DD Retention Lock** to disable this feature, or if you do not plan to use DD Retention Lock on this device, and click **Next**.

> Note: If you plan to use the REST API for features such as DD Cloud Tier policy creation and DD Retention Lock, you must additionally update the **NSR Data Domain** RAP resource with the Management username, password, port, and host. If these credentials and details are not specified in the RAP resource, then a validation error occurs.

The following figure provides an example of the **Select Storage Nodes** page.

Figure 15 Select Storage Nodes page



Device Configuration Wizard

Select Storage Nodes

Select a storage node to associate with each device. Select an existing storage node or create a new one. Select Fibre Channel options.

- ✓ Select the Device Type
- ✓ Data Domain Configuration Checklist
- ✓ Configuration Options
- ✓ Select Folders for Devices
- ✓ Configure Pools
- Select Storage Nodes
- SNMP Monitoring Options
- Review Configuration Settings
- Check Results

Storage Path	NetWorker Device Name	Pool	Storage Node	Dedicated	Fibre channel
/test123	dd_test123	103118341	dn-90dev-win02.mcb...		

Storage Node Options

● Use an existing storage node

dn-90dev-win02.mcblrdev.com

○ Create a new storage node

□ Dedicated Storage Node

Fibre Channel Options

Supported for DDOS 5.6 and higher only. Fibre Channel hostname is same for all devices.

□ Enable Fibre Channel for this device

Fibre Channel Host Name:

DD Retention Lock

DD Retention Lock ensures that archive data stored on a Data Domain system meets secure data retention requirements driven by governance policies.

☑ Enable DD Retention Lock

12. In the **Select SNMP Monitoring Options** page perform the following steps:

    a. In the **Data Domain SNMP Community String** field, type the name of the SNMP community string.

    > Note: If you do not know the name of the community, then clear the **Gather Usage Information** selection.

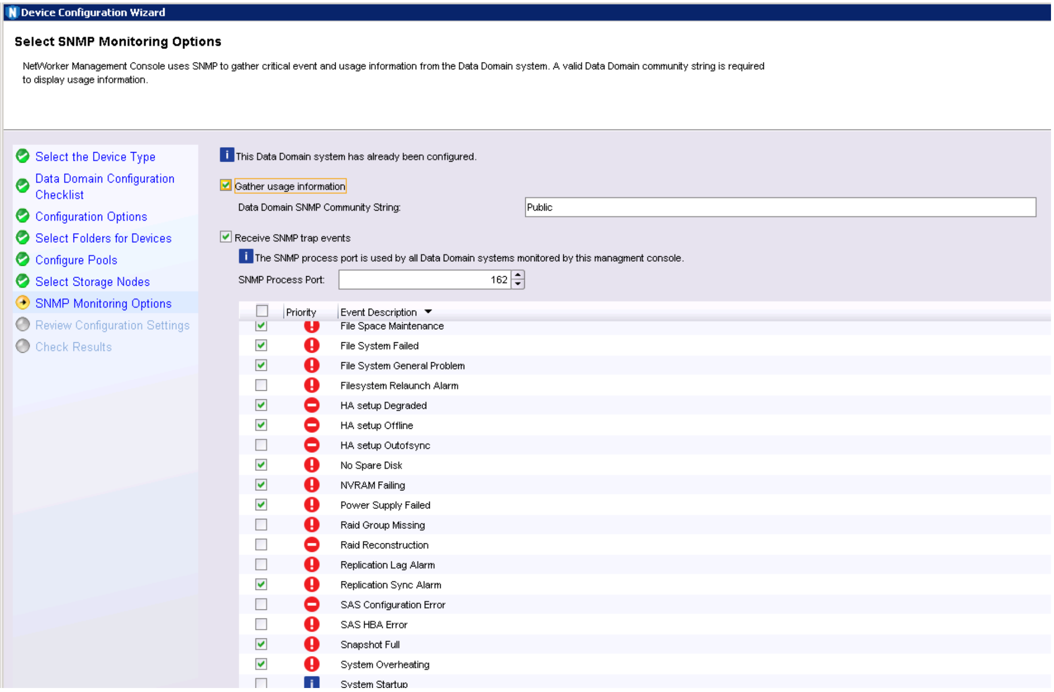
    b. With the **Receive SNMP trap events** option selected, specify the SNMP Process port used by the Data Domain system and select the events in which to monitor. **Use the Reset** to defaults option to reset the events in which to monitor back to the default settings.

    > Note: The default SNMP process port is 162.

    c. Click **Next**.

SNMP monitoring enables NMC to display the Data Domain system status and to list the backup and the recovery events. The monitoring feature also provides a launcher link for the Data Domain interface. The following figure provides an example of the **Select SNMP Monitoring Options** page.

Figure 16 Select SNMP Monitoring Options page



Device Configuration Wizard

Select SNMP Monitoring Options

NetWorker Management Console uses SNMP to gather critical event and usage information from the Data Domain system. A valid Data Domain community string is required to display usage information.

- ✓ Select the Device Type
- ✓ Data Domain Configuration Checklist
- ✓ Configuration Options
- ✓ Select Folders for Devices
- ✓ Configure Pools
- ✓ Select Storage Nodes
- → SNMP Monitoring Options
- ○ Review Configuration Settings
- ○ Check Results

ℹ This Data Domain system has already been configured.

☑ Gather usage information

Data Domain SNMP Community String: Public

☑ Receive SNMP trap events

ℹ The SNMP process port is used by all Data Domain systems monitored by this managment console.

SNMP Process Port: 162

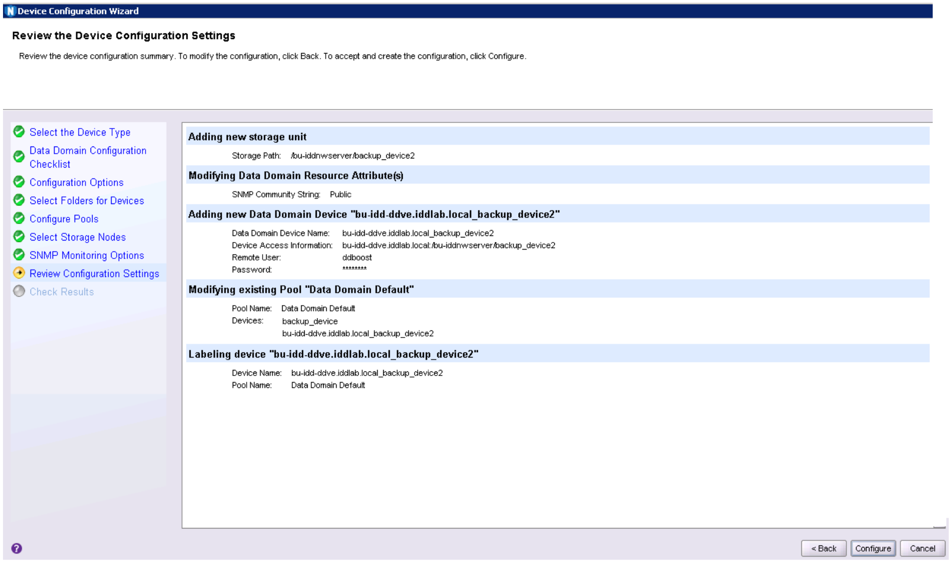
□	Priority	Event Description
☑	❗	File Space Maintenance
☑	❗	File System Failed
☑	❗	File System General Problem
□	❗	Filesystem Relaunch Alarm
☑	⛔	HA setup Degraded
☑	⛔	HA setup Offline
□	⛔	HA setup Outofsync
☑	❗	No Spare Disk
☑	❗	NVRAM Failing
☑	❗	Power Supply Failed
□	❗	Raid Group Missing
□	⛔	Raid Reconstruction
□	❗	Replication Lag Alarm
☑	❗	Replication Sync Alarm
□	⛔	SAS Configuration Error
□	❗	SAS HBA Error
☑	❗	Snapshot Full
☑	❗	System Overheating
□	ℹ	System Startup

13. On the **Review the Device Configuration Settings** page, review the configuration information and then click **Configure**.

    Note: The name that is listed as the SU is really the pathname for the device folder. The format is: *SU/ device_name*, where *SU* is the short hostname of the NetWorker server.

    The following figure provides an example of the **Review the Device Configuration Settings** page.

Figure 17 Review the Device Configuration Settings page



Device Configuration Wizard

Review the Device Configuration Settings

Review the device configuration summary. To modify the configuration, click Back. To accept and create the configuration, click Configure.

- ✓ Select the Device Type
- ✓ Data Domain Configuration Checklist
- ✓ Configuration Options
- ✓ Select Folders for Devices
- ✓ Configure Pools
- ✓ Select Storage Nodes
- ✓ SNMP Monitoring Options
- → Review Configuration Settings
- ○ Check Results

Adding new storage unit

Storage Path: /bu-iddnwserver/backup_device2

Modifying Data Domain Resource Attribute(s)

SNMP Community String: Public

Adding new Data Domain Device "bu-idd-ddve.iddlab.local_backup_device2"

Data Domain Device Name: bu-idd-ddve.iddlab.local_backup_device2
Device Access Information: bu-idd-ddve.iddlab.local:/bu-iddnwserver/backup_device2
Remote User: ddboost
Password: ********

Modifying existing Pool "Data Domain Default"

Pool Name: Data Domain Default
Devices: backup_device
bu-idd-ddve.iddlab.local_backup_device2

Labeling device "bu-idd-ddve.iddlab.local_backup_device2"

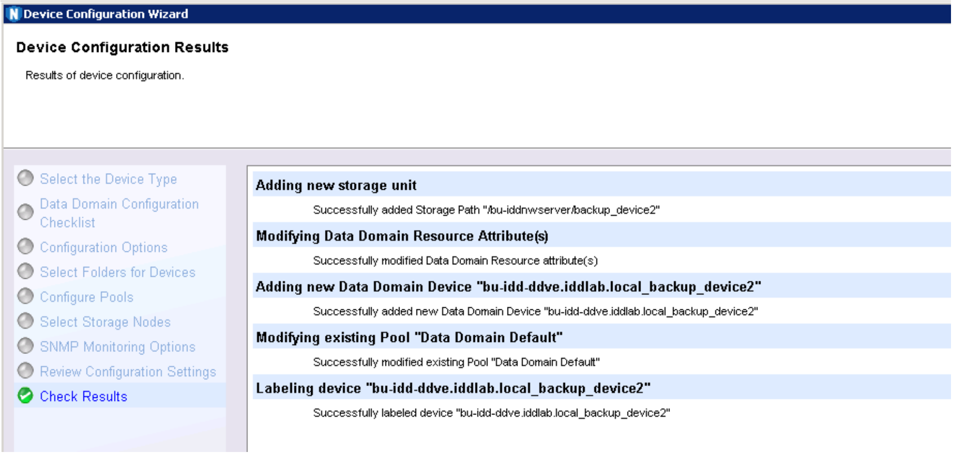
Device Name: bu-idd-ddve.iddlab.local_backup_device2
Pool Name: Data Domain Default

NetWorker configures, mounts, and labels the DD Boost device for the specified pool.

14. On the **Device Configuration Results** page, review the information, and then click **Finish**.

    The following figure provides an example of the **Device Configuration Results** page.

Figure 18 Device Configuration Results page


Device Configuration Wizard
Select the Device Type
Data Domain Configuration Checklist
Configuration Options
Select Folders for Devices
Configure Pools
Select Storage Nodes
SNMP Monitoring Options
Review Configuration Settings
Check Results

Device Configuration Results

Results of device configuration.

Adding new storage unit

Successfully added Storage Path "/bu-iddnwserver/backup_device2"

Modifying Data Domain Resource Attribute(s)

Successfully modified Data Domain Resource attribute(s)

Adding new Data Domain Device "bu-idd-ddve.iddlab.local_backup_device2"

Successfully added new Data Domain Device "bu-idd-ddve.iddlab.local_backup_device2"

Modifying existing Pool "Data Domain Default"

Successfully modified existing Pool "Data Domain Default"

Labeling device "bu-idd-ddve.iddlab.local_backup_device2"

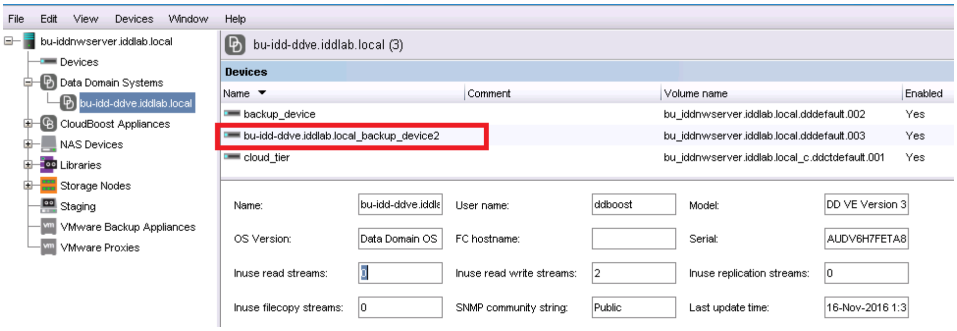
Successfully labeled device "bu-idd-ddve.iddlab.local_backup_device2"

Results

After the wizard successfully creates the device, the following changes appear in NMC:

- The **Data Domain Systems** window displays the new Data Domain device and the name of the volume. The following figure provides an example of the **Data Domain System** window with the new Data Domain device.

  Figure 19 Data Domain System window

  bu-idd-ddve.iddlab.local (3)

  Devices

Name	Comment	Volume name	Enabled
backup_device		bu_iddnwserver.iddlab.local.dddefault.002	Yes
bu-idd-ddve.iddlab.local_backup_device2		bu_iddnwserver.iddlab.local.dddefault.003	Yes
cloud_tier		bu_iddnwserver.iddlab.local_c.ddctdefault.001	Yes

Name:	bu-idd-ddve.iddla	User name:	ddboost	Model:	DD VE Version 3
OS Version:	Data Domain OS	FC hostname:		Serial:	AUDV6H7FETA8
Inuse read streams:	0	Inuse read write streams:	2	Inuse replication streams:	0
Inuse filecopy streams:	0	SNMP community string:	Public	Last update time:	16-Nov-2016 1:3

- If you configured a device for a Data Domain system that does not have previously configured NetWorker devices, NetWorker adds the Data Domain system as a managed host. The NMC **Enterprise** window provides you details about the Data Domain system.

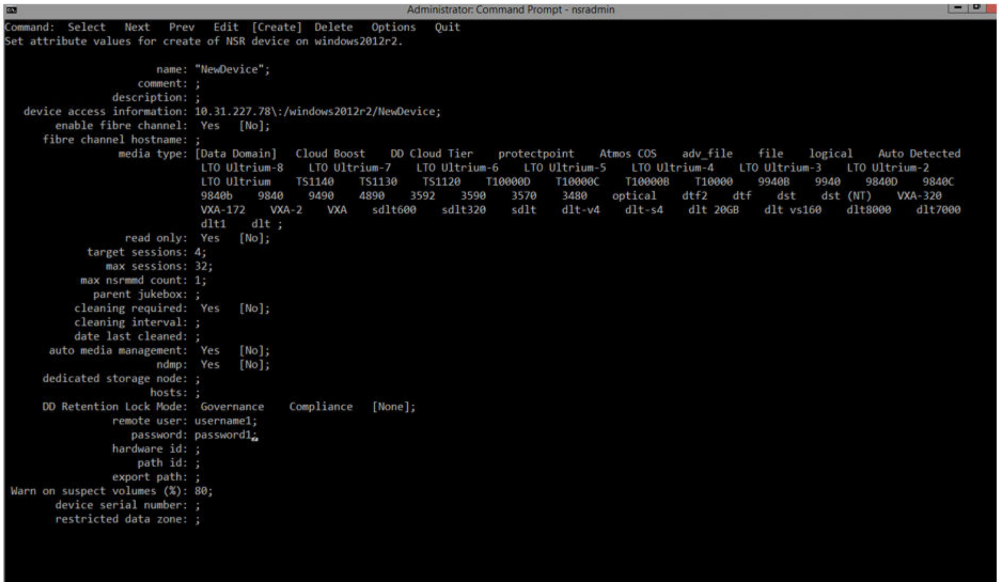
Configuring DD Boost devices with nsradmin

Use the `nsradmin` command to create or modify Data Domain devices, and to define the Data Domain system on the Networker server.

Procedure

1. Open the nsradmin tool in visual mode.
2. Select the **Create** option in the menu and select the type as **NSR device**. The following full screen appears with list of attributes to be configured for new device resource:

Figure 20 Attributes to be configured for new device resource



```
Command:  Select   Next   Prev   Edit  [Create]  Delete   Options   Quit
Set attribute values for create of NSR device on windows2012r2.

                         name: "NewDevice";
                      comment: ;
                  description: ;
      device access information: 10.31.227.78\:/windows2012r2/NewDevice;
          enable fibre channel:  Yes   [No];
        fibre channel hostname: ;
                    media type: [Data Domain]   Cloud Boost    DD Cloud Tier    protectpoint    Atmos COS    adv_file    file    logical    Auto Detected
                                 LTO Ultrium-8    LTO Ultrium-7    LTO Ultrium-6    LTO Ultrium-5    LTO Ultrium-4    LTO Ultrium-3    LTO Ultrium-2
                                 LTO Ultrium    TS1140    TS1130    TS1120    T10000D    T10000C    T10000B    T10000    9940B    9940    9840D    9840C
                                 9840b    9840    9490    4890    3592    3590    3570    3480    optical    dtf2    dtf    dst    dst (NT)    VXA-320
                                 VXA-172    VXA-2    VXA    sdlt600    sdlt320    sdlt    dlt-v4    dlt-s4    dlt 20GB    dlt vs160    dlt8000    dlt7000
                                 dlt1    dlt ;
                     read only:  Yes   [No];
               target sessions: 4;
                  max sessions: 32;
              max nsrmmd count: 1;
                parent jukebox: ;
             cleaning required:  Yes   [No];
             cleaning interval: ;
             date last cleaned: ;
         auto media management:  Yes   [No];
                          ndmp:  Yes   [No];
        dedicated storage node: ;
                         hosts: ;
        DD Retention Lock Mode:  Governance    Compliance   [None];
                   remote user: username1;
                      password: password1;
                   hardware id: ;
                       path id: ;
                   export path: ;
   Warn on suspect volumes (%): 80;
          device serial number: ;
            restricted data zone: ;
```

3. Provide the device name, device access information, username for the DD boost user (username filed) and password for the account . These are mandatory attributes to create a device resource.

   Device access information must be in the following form:

   `<DD IP>:<StorageUnitName>/<DeviceName>` where **Device Name** refers to the subfolder to be created within the storage unit.

   Note:

   - Device access information is parsed to get the storage unit and the device name.
   - If device with Mtree exists, then the `nsradmin` command displays the error `device already exist`.

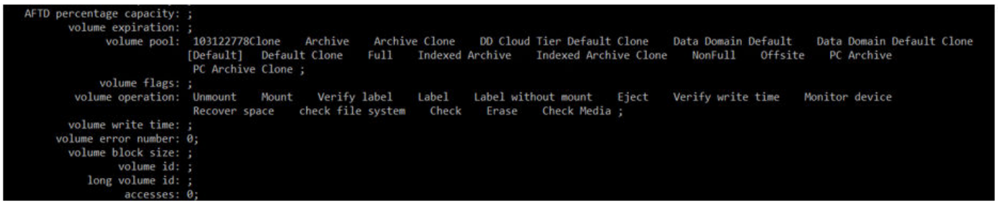
4. Select the media type as Data Domain.
5. In order to enable the SMT feature, set the **secure multi tenancy** attribute to **Yes**. If SMT is disabled, storage unit (Mtree) name must be named after the Networker server.
6. In order to use fibre channel, set **enable fibre channel** field to **Yes**.
7. Set the DD retention lock mode to either Governance or Compliance Mode by using the DD Retention Lock Mode field.To use DD Retention Lock, ensure the NSR Data Domain RAP resource exists with valid values set for the management attributes -Host, Port Username, and Password. This is set using the NSR Data Domain Resource. DD retention lock mode field is used to set to governance or compliance mode.
8. Use the escape key to create the new resource. Select **Yes** to do the same, otherwise select **No**.

   Note: If you click on **Yes**, device RAP Resource gets created along with the storage unit and device folder on the DD host. If storage node is not in ready state, `nsradmin` waits till it becomes available.

9. Click on the **Select** option which displays the types of resources available. Select the option **NSR Device**. It lists out all the devices that has been created and is available. Browse through the list using **Next** and **Previous**, once you find the device that you want to configure, click on the **Edit** option.

10. Selecting the pool in **Volume Pool** field. If you want to create a new Pool, select the pool using **NSR Pool** resource and select the **Create** option. Once it is complete revert back to the current device Window (follow Step 9) and select the new pool that has just been created.

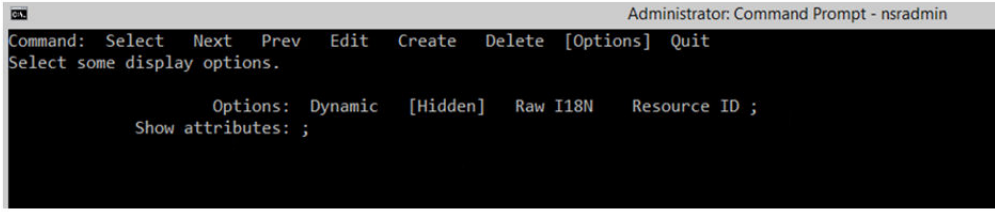
    Figure 21 Configuring the media pool information

    ```
     AFTD percentage capacity: ;
            volume expiration: ;
                  volume pool:  103122778Clone    Archive    Archive Clone    DD Cloud Tier Default Clone    Data Domain Default    Data Domain Default Clone
                               [Default]   Default Clone    Full    Indexed Archive    Indexed Archive Clone    NonFull    Offsite    PC Archive
                                PC Archive Clone ;
                 volume flags: ;
             volume operation:  Unmount    Mount    Verify label    Label    Label without mount    Eject    Verify write time    Monitor device
                                Recover space    check file system    Check    Erase    Check Media ;
            volume write time: ;
          volume error number: 0;
            volume block size: ;
                    volume id: ;
               long volume id: ;
                     accesses: 0;
    ```

11. In order to configure the volume operations, enable the hidden attribute in **Options** section (If it is disabled).

    Figure 22 Enabling the hidden attribute

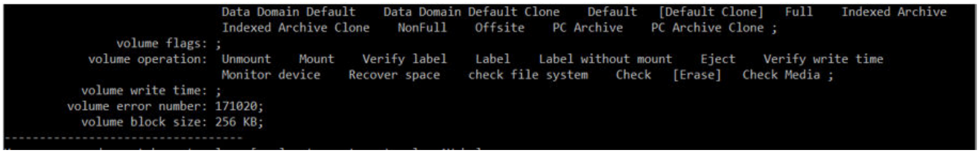
    ```
    Administrator: Command Prompt - nsradmin
    Command:  Select   Next   Prev   Edit   Create   Delete  [Options]  Quit
    Select some display options.

                       Options:  Dynamic   [Hidden]   Raw I18N   Resource ID ;
             Show attributes: ;
    ```

12. Select options available in **Volume operation** field in order to label, mount and perform other volume operations on the device. Operations have to be performed one at a time. Labeling and mounting of the device can also be performed by running the command. `nsrmm -s <server_name> -v -y -m -b <pool_name> -l -f <device_name>`.

13. In order to permanently erase all data and remove media and index information erase volume operation has to be performed.

    Figure 23 Performing erase volume operation

    ```
                                 Data Domain Default    Data Domain Default Clone    Default   [Default Clone]   Full    Indexed Archive
                                 Indexed Archive Clone    NonFull    Offsite    PC Archive    PC Archive Clone ;
                 volume flags: ;
             volume operation:  Unmount    Mount    Verify label    Label    Label without mount    Eject    Verify write time
                                Monitor device    Recover space    check file system    Check   [Erase]   Check Media ;
            volume write time: ;
          volume error number: 171020;
            volume block size: 256 KB;
    ---------------------------------
    ```

14. Select **Delete** from the menu to delete the device RAP resource. Delete operation would also need device to be unmounted and removed as a target device from the corresponding NSR Pool resource.

Configuring NetWorker for Cloud Tier devices

To configure Cloud Tier devices, use the Device Configuration Wizard (DCW) or create and configure the devices manually. It is recommended that you use DCW to create Cloud Tier devices.

> Note: Cloning of saveset is not supported from a non-Data Domain device to a DD Cloud Tier device. In RPS Enabled mode, cloning fails with an error “failed to get mmd reservation with err: Clone saveset(s) operation from a non-Data Domain device to a DD Cloud Tier device is not supported”. In RPS Disabled Mode, cloning might pass, but it is still an unsupported configuration.

Note: To use Data Domain with NetWorker, the NetWorker server hostname should be in lower case. Data Domain functions with lowercase and DD Cloud tier operations fails if it is mixed case.

Configuring NetWorker devices for DD Cloud Tier

Use the Device Configuration Wizard to configure NetWorker devices for the DD Cloud Tier devices.

Before you begin

The Data Domain devices that contains the source backup data must reside on the same mtree as the DD Cloud Tier device that will store the clone data. The storage node that manages the Data Domain devices must be a NetWorker 19.2 storage node.

Note: NetWorker uses an app-based policy to clone data to a DD Cloud Tier device. If a non-app-based policy exists on the mtree where the DD Cloud Tier device resides, NetWorker will delete the non-app-based policy and create an app-based policy during the label operation.

Procedure

1. Log in to the NMC GUI as an administrator of the NetWorker server.
2. On the taskbar, click the **Enterprise** icon .
3. In the navigation tree, highlight a host:

   a. Right-click **NetWorker**.

   b. Select **Launch Application**. The **NetWorker Administration** window appears.
4. On the taskbar, click the **Devices** button .
5. In the left navigation pane:

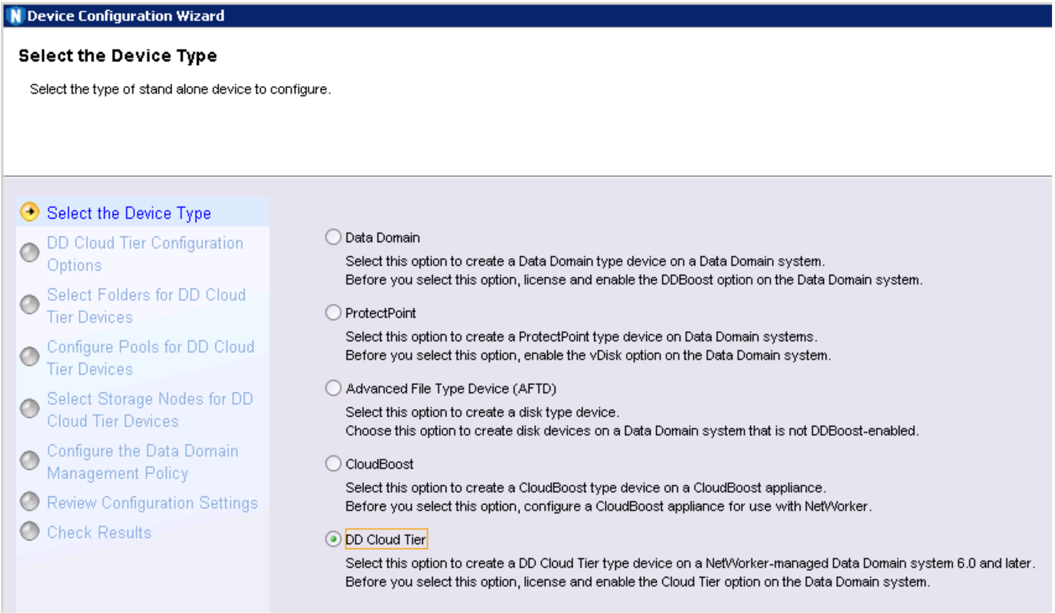
   a. Right-click **Data Domain Systems**.

   b. Select **New Device Wizard**.

   Note: To modify completed wizard pages, click the links in the steps panel. The number of steps may vary according to the type of configuration chosen.
6. In the **Select the Device Type** page, select the **DD Cloud Tier** device type, and then click **Next**.

   The following figure provides an example of the **Select the Device Type** page.

Figure 24 Select the Device Type page



Device Configuration Wizard
Select the Device Type
Select the type of stand alone device to configure.
Select the Device Type
DD Cloud Tier Configuration Options
Select Folders for DD Cloud Tier Devices
Configure Pools for DD Cloud Tier Devices
Select Storage Nodes for DD Cloud Tier Devices
Configure the Data Domain Management Policy
Review Configuration Settings
Check Results

○ Data Domain
Select this option to create a Data Domain type device on a Data Domain system.
Before you select this option, license and enable the DDBoost option on the Data Domain system.

○ ProtectPoint
Select this option to create a ProtectPoint type device on Data Domain systems.
Before you select this option, enable the vDisk option on the Data Domain system.

○ Advanced File Type Device (AFTD)
Select this option to create a disk type device.
Choose this option to create disk devices on a Data Domain system that is not DDBoost-enabled.

○ CloudBoost
Select this option to create a CloudBoost type device on a CloudBoost appliance.
Before you select this option, configure a CloudBoost appliance for use with NetWorker.

● DD Cloud Tier
Select this option to create a DD Cloud Tier type device on a NetWorker-managed Data Domain system 6.0 and later.
Before you select this option, license and enable the Cloud Tier option on the Data Domain system.

7. In the **DD Cloud Tier Configuration Options** page, perform the following steps:

   a. From the **Select an existing Data Domain** list, select the Data Domain host.

   b. In the **DD Boost Credentials** section, type the username for the DD Boost user in the **DD Boost Username** field.

   c. In the **Secure Multi-Tenancy** section, to use only DD Boost devices in secure Storage Units (SUs), select **Configure Secure Multi-Tenancy (SMT)**, and then perform one of the following tasks:

      - To use an existing storage unit (SU), select **Use an existing secure storage unit**, and then select the SU.
      - To create a SU, select **Create a new secure storage unit**, and then specify the name of the SU.

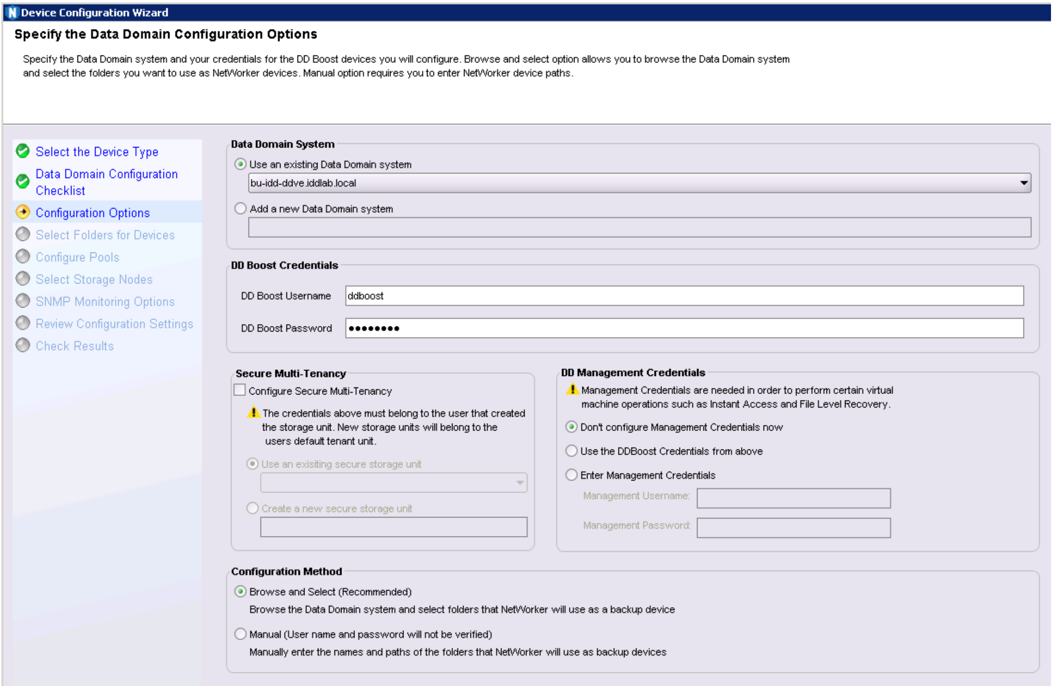
      Note: SMT restricts access of each SU to one owner according to the provided DD Boost credentials.

   d. In the **Configuration Method** field, select **Browse and Select**, and then click **Next**.

      Note: If you do not configure the SMT option, the wizard will create an SU for you on the Data Domain system, and name the SU after the shortname of the NetWorker server.

   The following figure provides an example of the **DD Cloud Tier Configuration Options** page.

Figure 25 DD Cloud Tier Configuration Options page



Device Configuration Wizard

Specify the Data Domain Configuration Options

Specify the Data Domain system and your credentials for the DD Boost devices you will configure. Browse and select option allows you to browse the Data Domain system and select the folders you want to use as NetWorker devices. Manual option requires you to enter NetWorker device paths.

- ✓ Select the Device Type
- ✓ Data Domain Configuration Checklist
- ➔ Configuration Options
- Select Folders for Devices
- Configure Pools
- Select Storage Nodes
- SNMP Monitoring Options
- Review Configuration Settings
- Check Results

Data Domain System

● Use an existing Data Domain system

bu-idd-ddve.iddlab.local

○ Add a new Data Domain system

DD Boost Credentials

DD Boost Username: ddboost

DD Boost Password: ••••••••

Secure Multi-Tenancy

□ Configure Secure Multi-Tenancy

⚠ The credentials above must belong to the user that created the storage unit. New storage units will belong to the users default tenant unit.

● Use an exisiting secure storage unit

○ Create a new secure storage unit

DD Management Credentials

⚠ Management Credentials are needed in order to perform certain virtual machine operations such as Instant Access and File Level Recovery.

● Don't configure Management Credentials now

○ Use the DDBoost Credentials from above

○ Enter Management Credentials

Management Username:

Management Password:

Configuration Method

● Browse and Select (Recommended)

Browse the Data Domain system and select folders that NetWorker will use as a backup device

○ Manual (User name and password will not be verified)

Manually enter the names and paths of the folders that NetWorker will use as backup devices

8. In the **Select the Folders to use as DD Cloud Tier Device** page, configure a device in the same mtree as the Data Domain backup device:

   a. Select the Data Domain system, and then click **New Folder**.

   A new folder appears in the navigation tree. This folder is the new device.

   > Note: The navigation tree does not show the SU folder under the Data Domain system folder. However, the SU folder is verifiable in the final **Review Configurations Settings** wizard page. The wizard names the SU folder after the short hostname of the NetWorker server and places the devices that you create into this SU folder.

   b. Type a name for the new folder, and then select the checkbox next to the folder or device name.

   The Device table displays the full NetWorker device name, the storage pathname, and details about the device.

   > Note: The device name refers to the subfolder created within the SU. The folder path must not contain other folders deeper than these device folders.

   c. (Optional) To rename a DD Cloud Tier device as it appears in NMC:

      a. Select the device in the table.

      b. Type a new name in the **NetWorker Device Name** field.

      c. Do not use special characters other than dot (.) and underscore (_).

      d. The **Storage Path** field remains unchanged.

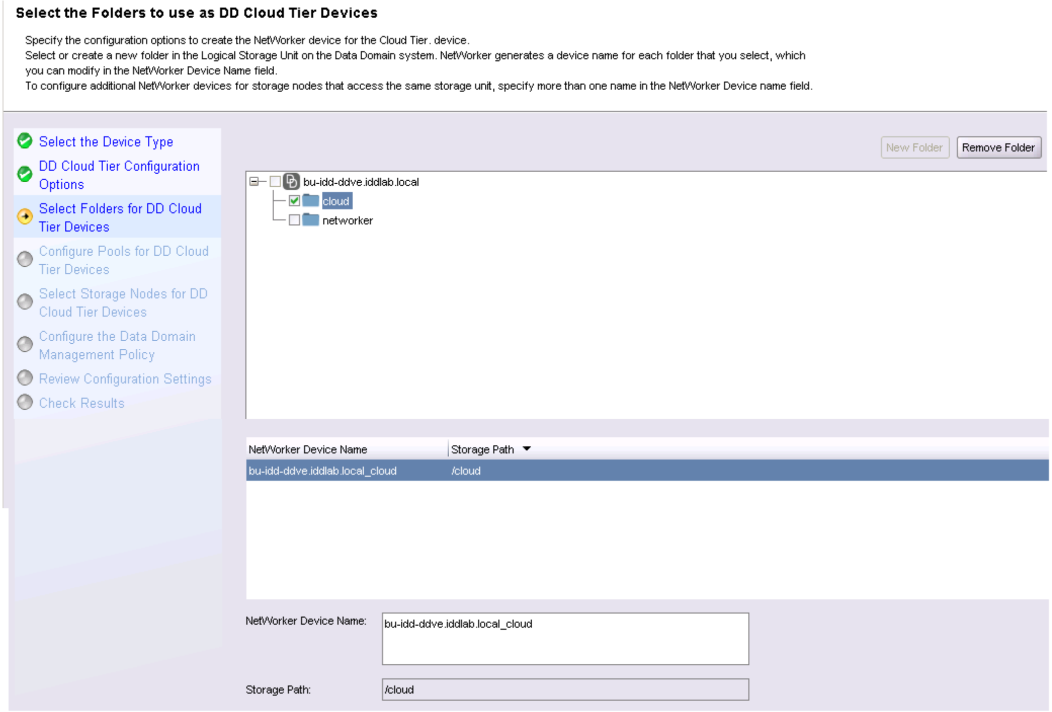
   > Note: Implicit in the SU folder pathname on the Data Domain system is the hidden mount point folders`/data/col1`. Do not modify this folder structure, which all NetWorker server hosts use. The final wizard page, **Review Configurations**

Settings, shows the complete location.
The `/backup` folder stores NFS service data. The clients that are configured for NFS access can view, change, and delete the `/data/col1` directory that contains the DD Boost devices. If you use NFS devices, you can avoid the risk of potential interference by using alternative path names.

d. Click **Next**.

The following figure provides an example of the **Select the Folders to use as DD Cloud Tier Device** page.

Figure 26 Select the Folders to use as DD Cloud Tier Device page



Select the Folders to use as DD Cloud Tier Devices

Specify the configuration options to create the NetWorker device for the Cloud Tier. device.
Select or create a new folder in the Logical Storage Unit on the Data Domain system. NetWorker generates a device name for each folder that you select, which you can modify in the NetWorker Device Name field.
To configure additional NetWorker devices for storage nodes that access the same storage unit, specify more than one name in the NetWorker Device name field.

Select the Device Type
DD Cloud Tier Configuration Options
Select Folders for DD Cloud Tier Devices
Configure Pools for DD Cloud Tier Devices
Select Storage Nodes for DD Cloud Tier Devices
Configure the Data Domain Management Policy
Review Configuration Settings
Check Results
New Folder
Remove Folder
bu-idd-ddve.iddlab.local
☑ cloud
□ networker

NetWorker Device Name	Storage Path
bu-idd-ddve.iddlab.local_cloud	/cloud

NetWorker Device Name: bu-idd-ddve.iddlab.local_cloud

Storage Path: /cloud

9. In the **Configure a Pool for the DD Cloud Tier Device** page, perform the following steps:

   a. Select **Configure Media Pools for Devices**.

   b. In the **Pool** section, perform either of the following steps:

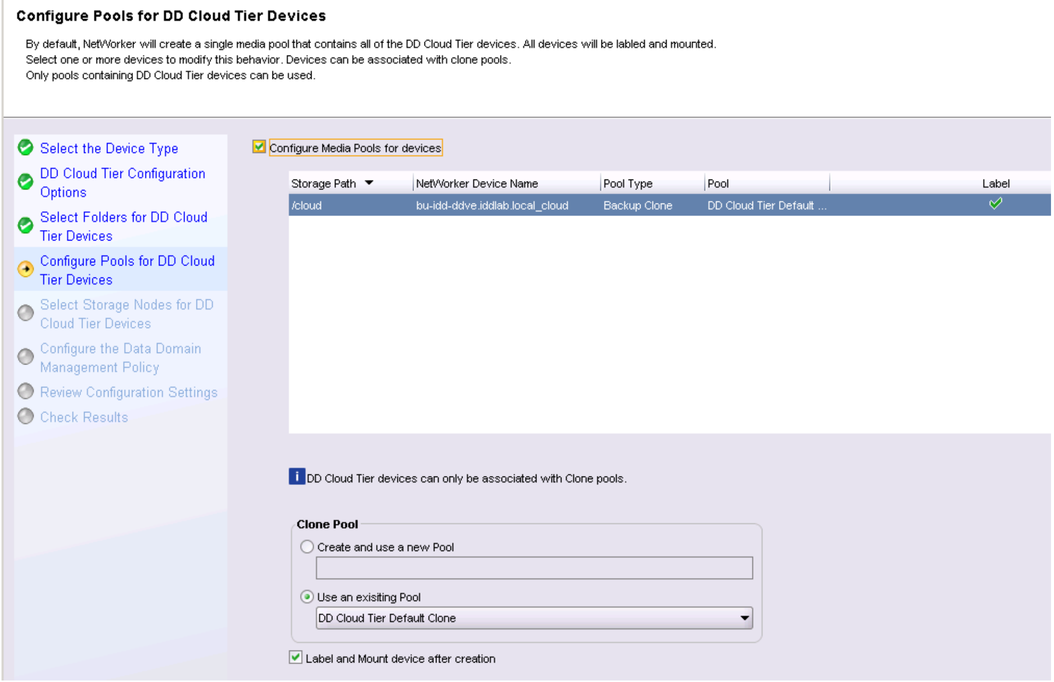
   > **Note:** The pool that you select or create must contain only Cloud Tier devices. NMC lists pools of the type Backup Clone that contain only DD Cloud Tier devices.

   c. Leave the **Label and Mount device after creation** option selected.

   d. Click **Next**.

   The following figure provides an example of the**Configure a Pool for the DD Cloud Tier Device** page.

Figure 27 Configure a Pool for the DD Cloud Tier Device page



Configure Pools for DD Cloud Tier Devices

By default, NetWorker will create a single media pool that contains all of the DD Cloud Tier devices. All devices will be labled and mounted.
Select one or more devices to modify this behavior. Devices can be associated with clone pools.
Only pools containing DD Cloud Tier devices can be used.

Select the Device Type
DD Cloud Tier Configuration Options
Select Folders for DD Cloud Tier Devices
Configure Pools for DD Cloud Tier Devices
Select Storage Nodes for DD Cloud Tier Devices
Configure the Data Domain Management Policy
Review Configuration Settings
Check Results

☑ Configure Media Pools for devices

Storage Path	NetWorker Device Name	Pool Type	Pool	Label
/cloud	bu-idd-ddve.iddlab.local_cloud	Backup Clone	DD Cloud Tier Default ...	✓

DD Cloud Tier devices can only be associated with Clone pools.

Clone Pool

○ Create and use a new Pool

● Use an exisitng Pool

DD Cloud Tier Default Clone

☑ Label and Mount device after creation

10. In the **Select the Storage Nodes for the DD Cloud Tier Device** page, perform the following steps:

    a. In the **Storage Node Options** section, select the storage node that manages the device.

    - To use an existing storage node on the NetWorker server, select **Use an existing storage node**.
    - To use a new storage node:

        a. Select **Create a new storage node**.

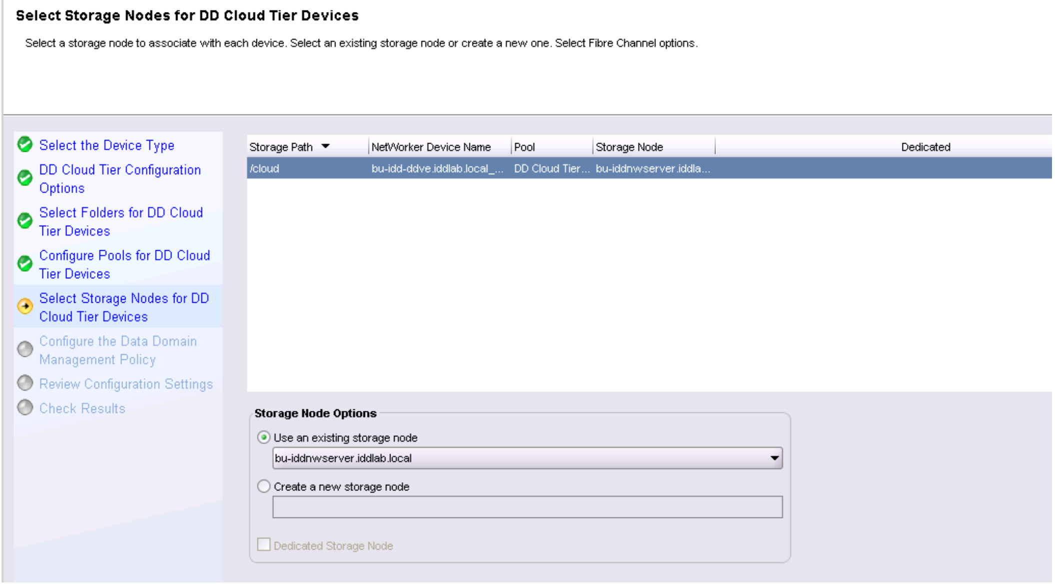
        b. Type the hostname of a storage node host.

        c. If the new Storage Node is also a Dedicated Storage Node, select **Dedicated Storage Node**.

    b. Click **Next**.

    The following figure provides an example of the **Select the Storage Nodes for the DD Cloud Tier Device** page.

Figure 28 Select the Storage Nodes for the DD Cloud Tier Device page



Select Storage Nodes for DD Cloud Tier Devices

Select a storage node to associate with each device. Select an existing storage node or create a new one. Select Fibre Channel options.

Select the Device Type
DD Cloud Tier Configuration Options
Select Folders for DD Cloud Tier Devices
Configure Pools for DD Cloud Tier Devices
Select Storage Nodes for DD Cloud Tier Devices
Configure the Data Domain Management Policy
Review Configuration Settings
Check Results

Storage Path	NetWorker Device Name	Pool	Storage Node	Dedicated
/cloud	bu-idd-ddve.iddlab.local_...	DD Cloud Tier...	bu-iddnwserver.iddla...	

Storage Node Options

● Use an existing storage node

bu-iddnwserver.iddlab.local

○ Create a new storage node

□ Dedicated Storage Node

11. In the **Configure the Data Domain Management Policy** page, perform the following steps:

    a. In the **Data Domain Host** field, specify the host name of the Data Domain system.

    b. In the **Admin User** field, specify the username for a Data Domain user that has admin access. For example, sysadmin.

    c. In the **Admin Password** field, specify the password of the management user.

    d. In the **Port** field, specify the management port. By default, the port is 3009.

    e. In the **CA Certificate** field, click **Pull Certificate**.

       The Device wizard contacts the Data Domain system and displays the certificate in the **Certificate** field.

       The **Management Certificates** window appears.

    f. From the **Select Certificate** list, select the certificate.

    g. In the **Certificate Details** field, review the certificate, and if the certificate is correct, click **I Trust**.

       The **CA Certificate** field on the **Configure the Data Domain Management Policy** window displays the certificate.

    h. In the **Cloud Unit Name** field, specify the name of the cloud unit that you created on the Data Domain system.

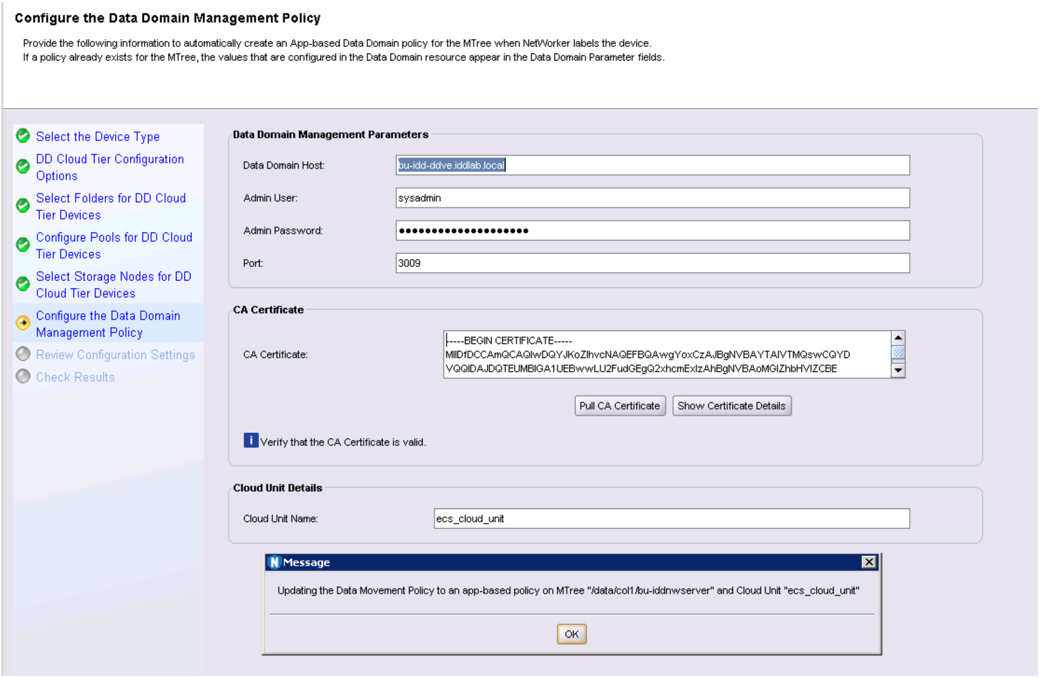
       Note: To view a list of cloud units that are configured on a Data Domain system, from the Data Domain CLI, type `cloud unit list`.

    i. Click **Next**.

    j. On the confirmation window, review the details, and then click **OK**.

The following figure provides an example of the **Configure the Data Domain Management Policy** page.

Figure 29 Configure the Data Domain Management Policy page


Select the Device Type
DD Cloud Tier Configuration Options
Select Folders for DD Cloud Tier Devices
Configure Pools for DD Cloud Tier Devices
Select Storage Nodes for DD Cloud Tier Devices
Configure the Data Domain Management Policy
Review Configuration Settings
Check Results
Pull CA Certificate
Show Certificate Details
OK

Configure the Data Domain Management Policy

Provide the following information to automatically create an App-based Data Domain policy for the MTree when NetWorker labels the device.
If a policy already exists for the MTree, the values that are configured in the Data Domain resource appear in the Data Domain Parameter fields.

Data Domain Management Parameters

Data Domain Host: bu-idd-ddve.iddlab.local

Admin User: sysadmin

Admin Password: ••••••••••••••••••••

Port: 3009

CA Certificate

CA Certificate:

```
-----BEGIN CERTIFICATE-----
MIIDfDCCAmQCAQIwDQYJKoZIhvcNAQEFBQAwgYoxCzAJBgNVBAYTAlVTMQswCQYD
VQQIDAJDQTEUMBIGA1UEBwwLU2FudGEgQ2xhcmExIzAhBgNVBAoMGlZhbHVIZCBE
```

Verify that the CA Certificate is valid.

Cloud Unit Details

Cloud Unit Name: ecs_cloud_unit

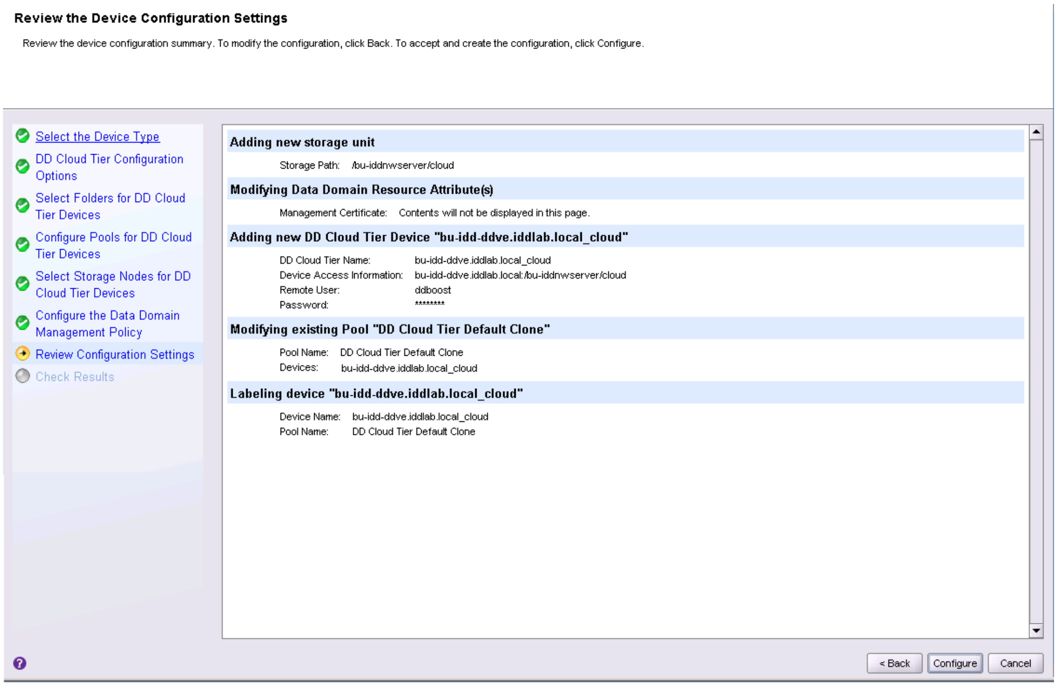
Message

Updating the Data Movement Policy to an app-based policy on MTree "/data/col1/bu-iddnwserver" and Cloud Unit "ecs_cloud_unit"

12. On the **Review the Device Configuration** page:

    The following figure provides an example of the **Review the Device Configuration** page.

Figure 30 Review the Device Configuration page


Select the Device Type
DD Cloud Tier Configuration Options
Select Folders for DD Cloud Tier Devices
Configure Pools for DD Cloud Tier Devices
Select Storage Nodes for DD Cloud Tier Devices
Configure the Data Domain Management Policy
Review Configuration Settings
Check Results
< Back
Configure
Cancel

Review the Device Configuration Settings

Review the device configuration summary. To modify the configuration, click Back. To accept and create the configuration, click Configure.

Adding new storage unit

Storage Path: /bu-iddnwserver/cloud

Modifying Data Domain Resource Attribute(s)

Management Certificate: Contents will not be displayed in this page.

Adding new DD Cloud Tier Device "bu-idd-ddve.iddlab.local_cloud"

DD Cloud Tier Name: bu-idd-ddve.iddlab.local_cloud
Device Access Information: bu-idd-ddve.iddlab.local:/bu-iddnwserver/cloud
Remote User: ddboost
Password: ********

Modifying existing Pool "DD Cloud Tier Default Clone"

Pool Name: DD Cloud Tier Default Clone
Devices: bu-idd-ddve.iddlab.local_cloud

Labeling device "bu-idd-ddve.iddlab.local_cloud"

Device Name: bu-idd-ddve.iddlab.local_cloud
Pool Name: DD Cloud Tier Default Clone

13. On the **Check results** page:

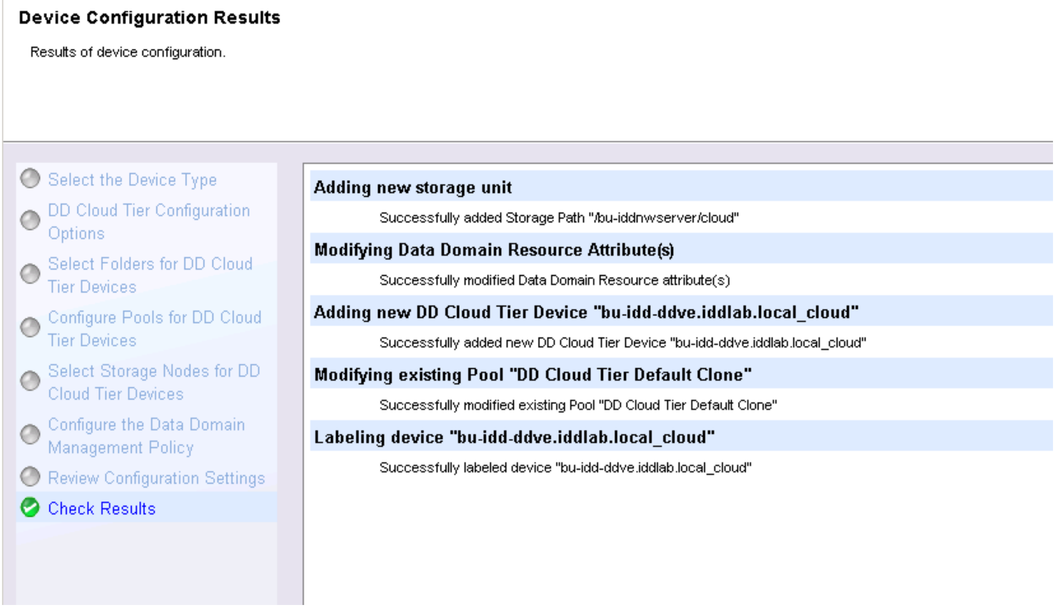
a. Review whether the devices were successfully configured or if any messages appeared.

b. Click **Finish**.

c. To change any of the settings, click **Back** to the correct wizard page.

The following figure provides an example of the **Check results** page.

Figure 31 Check results page



Device Configuration Results

Results of device configuration.

Select the Device Type
DD Cloud Tier Configuration Options
Select Folders for DD Cloud Tier Devices
Configure Pools for DD Cloud Tier Devices
Select Storage Nodes for DD Cloud Tier Devices
Configure the Data Domain Management Policy
Review Configuration Settings
Check Results

Adding new storage unit

Successfully added Storage Path "/bu-iddnwserver/cloud"

Modifying Data Domain Resource Attribute(s)

Successfully modified Data Domain Resource attribute(s)

Adding new DD Cloud Tier Device "bu-idd-ddve.iddlab.local_cloud"

Successfully added new DD Cloud Tier Device "bu-idd-ddve.iddlab.local_cloud"

Modifying existing Pool "DD Cloud Tier Default Clone"

Successfully modified existing Pool "DD Cloud Tier Default Clone"

Labeling device "bu-idd-ddve.iddlab.local_cloud"

Successfully labeled device "bu-idd-ddve.iddlab.local_cloud"

14. On the **Review the Device Configuration** page:

    a. Review the settings.

    b. Click **Configure**.

15. On the **Check results** page:

    a. Review whether the devices were successfully configured or if any messages appeared.

    b. Click **Finish**.

    c. To change any of the settings, click **Back** to the correct wizard page.

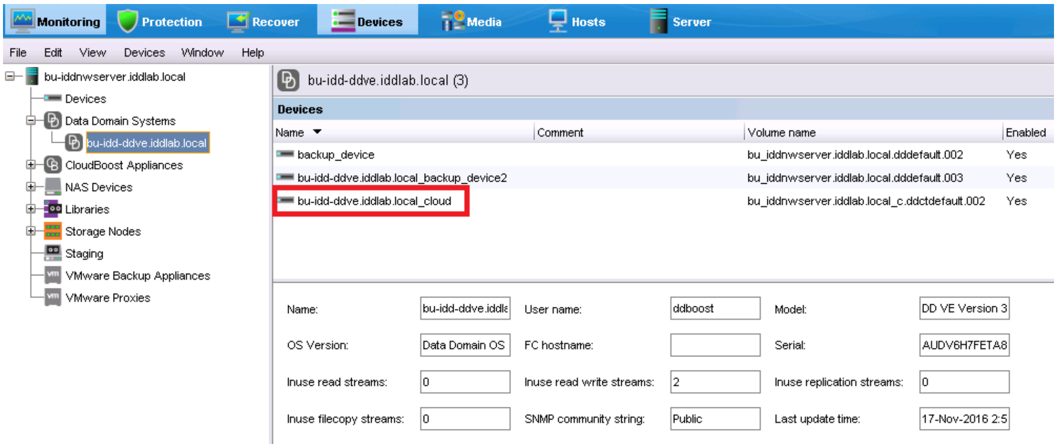
Results

The Device Configuration wizard performs the following tasks:

- Deletes existing time-based policies on the Data Domain system.
- Creates the app-based policy on the Data Domain system during the device label operation.
- Creates the new NetWorker device for the DD Cloud Tier device.

The following figure provides a example of the Data Domain devices window with a DD Cloud Tier device.

Figure 32 Device window with a DD Cloud Tier device



bu-idd-ddve.iddlab.local (3)

Devices

Name	Comment	Volume name	Enabled
backup_device		bu_iddnwserver.iddlab.local.dddefault.002	Yes
bu-idd-ddve.iddlab.local_backup_device2		bu_iddnwserver.iddlab.local.dddefault.003	Yes
bu-idd-ddve.iddlab.local_cloud		bu_iddnwserver.iddlab.local_c.ddctdefault.002	Yes

Name:	bu-idd-ddve.iddl	User name:	ddboost	Model:	DD VE Version 3
OS Version:	Data Domain OS	FC hostname:		Serial:	AUDV6H7FETA8
Inuse read streams:	0	Inuse read write streams:	2	Inuse replication streams:	0
Inuse filecopy streams:	0	SNMP community string:	Public	Last update time:	17-Nov-2016 2:5

Configuring a Cloud Tier device manually

It is recommended that you use the Device Configuration Wizard to add a Cloud Tier device to the NetWorker datazone. You can modify the Device resource that the wizard creates to modify the devices, and perform the tasks in the following sections.

Before you begin

Create the device folder on the Data Domain Storage Unit (SU).

About this task

To create a new Cloud Tier device, complete the following steps in the **Devices** window.

Procedure

1. In the left navigation pane, right-click **Data Domain systems**, select **Properties**, and then in the **Access** section, specify the following information:

   a. In the **Data Domain Host** field, specify the host name of the Data Domain system.

   b. In the **Admin User** field, specify the username for a Data Domain user that has admin access. For example, sysadmin.

   c. In the **Admin Password** field, specify the password of the management user.

   d. In the **Port** field, specify the management port. By default, the port is 3009.

   e. In the **Cloud Unit Name** field, specify the name of the cloud unit that you created on the Data Domain system.

      Note: To view a list of cloud units that are configured on a Data Domain system, from the Data Domain CLI, type `cloud unit list`.

   f. In the **Management Certificate** field, paste the management certificate, from the Data Domain system.

   g. Click **OK**.

   NetWorker updates the Data Domain resource but does not validate the values with the Data Domain system to ensure accuracy.

2. In the left navigation pane, right-click **Devices**, and then and select **New Device Properties**.

3. On the **General** tab, identify the Cloud Tier device by typing its name and access information:

ⓘ **Note:** Multiple devices can share a single volume. Configuring volume sharing on multiple devices provides details.

a. In the **Name** field, type a name for the Cloud Tier device.

   For example:

   ```
   ct_1
   ```

   If you configure the device on a separate storage node host that is not the NetWorker server host, it is a remote device. Specify the **Name** field in the following format:

   ```
   rd=remote_storagenode_hostname:device_name
   ```

   For example:

   ```
   rd=dzone1_sn2:ct_1
   ```

b. In the **Device access information** field, type the Data Domain hostname followed by a colon and the path to the device folder.

   If you are configuring a device with secure multi-tenancy (SMT) protection, the device folder must reside in a password-protected tenant unit on the Data Domain.

   Use the following format:

   DD_hostname:/ DD_storage_unit_name/ device_name

   where, as a best practice, *DD_storage_unit_name* is the NetWorker server name, and *device_name* is a name for the device, which appears as a folder.

   For example, the following figure uses the following name:

   ddr1:/dzone1/ct_1

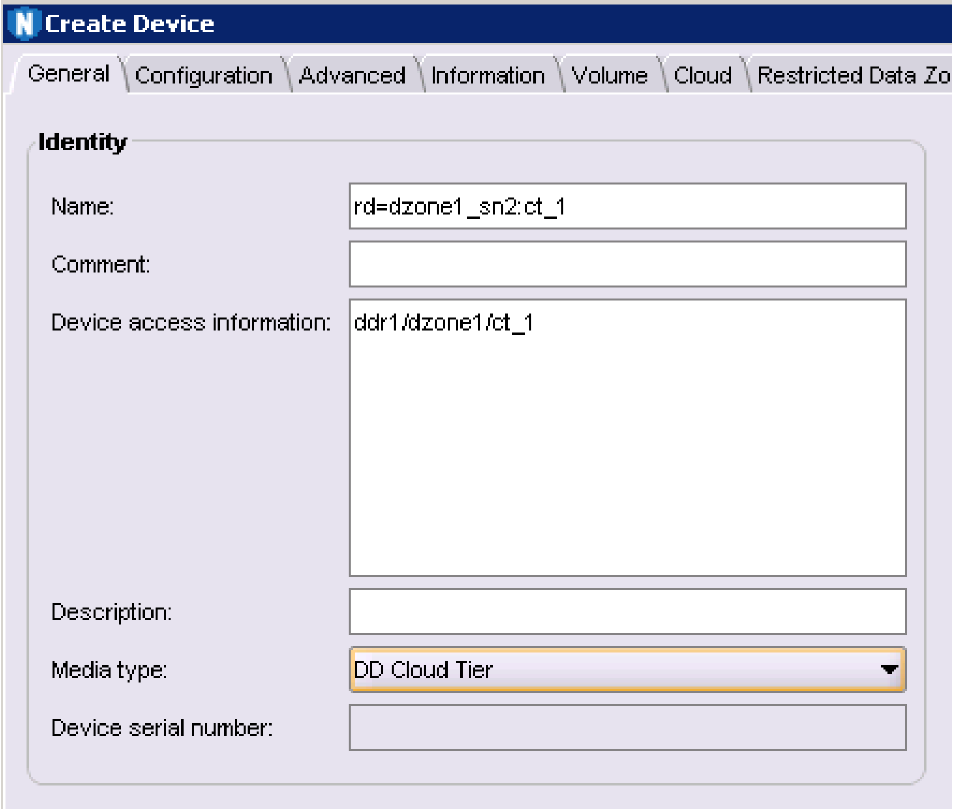
   NetWorker does not limit the number device folders that you can create, but the **Device access information** field accepts one device folder only. Do not create any folders within a device folder.

   ⓘ **Note:** Implicit in this pathname is the hidden mount point folder `/data/col1`. Do not modify this folder structure, which all NetWorker servers use.

c. From the **Media type** list, select **DD Cloud Tier**.

The following figure provides an example of the **General** tab for a Cloud Tier device.

Figure 33 Example of the General tab configuration properties for a Cloud Tier device



Create Device

Identity

Name: rd=dzone1_sn2:ct_1

Comment:

Device access information: ddr1/dzone1/ct_1

Description:

Media type: DD Cloud Tier

Device serial number:

4. On the **Configuration** tab, in the **Save Sessions** area, in the **Remote user** and **Password** fields, type the DD Boost username and password, respectively.

   You can only define one DD Boost (OST) user. All NetWorker storage nodes and servers that access the Data Domain system must use the same username and password.

   ⓘ Note: Avoid changing the user of an existing device with a labeled volume. The new user will not have write permission to the files and directories that are created by the previous user and cannot re-label the volume. Create a device for the new user.

5. To save the device settings click **OK**.

   The NetWorker **Administration** window displays the Data Domain system and details of the Cloud Tier device.

(Optional) Creating a Cloud Tier device pool

NetWorker provides you with a preconfigured media pool named DD Cloud Tier Clone that you can use for Cloud Tier devices. Optionally, you can create a new clone pool for Cloud Tier devices.

Procedure

1. In the **Administration** window, click **Media**.
2. In the left pane, select **Media Pools**.
3. From the **File** menu, select **New**.
4. On the General tab, perform the following configuration tasks:

   a. In the **Name** field, specify a descriptive name for the pool.

   b. From the **Pool type** list, select **Backup Clone**.

If a pool other than Backup Clone is used for a DD Cloud Tier device, the following error message appears when you attempt to label the device:

```
Pool <pool name> is of type 'Backup. A DD Cloud Tier device must belong
to a pool of type 'Backup Clone'.
```

c. From the **Label template** list, select **DD Cloud Tier Default Clone**.

5. On the **Selection Criteria** tab, perform the following configuration tasks:

   a. (Optional) To restrict the devices associated with the pool, from the Device box, select the Cloud Tier devices.

   > **Note:** Select devices that reside on the same mtree as the Data Domain devices that contain the source backup data.

   b. From the **Media type required** drop down, select **DD Cloud Tier**.

6. Click **OK**.

Labeling and mounting Cloud Tier devices

It is recommended that you use the Device Configuration Wizard to create a Data Domain device, which automatically labels and mounts the device. The following procedure describes the alternative manual method.

About this task

> **Note:** NetWorker uses an app-based policy to clone data to a DD Cloud Tier device. If a non-app-based policy exists on the mtree where the DD Cloud Tier device resides, NetWorker will delete the non-app-based policy and create an app-based policy during the label operation.

Procedure

1. In the **NetWorker Administration** window, click **Devices**.
2. In the left navigation pane, select **Data Domain Systems**.
3. In the right pane, right-click the Cloud Tier device, and click **Label**.
4. On the **Label** window, from the **Pools** list, select the Cloud Tier clone pool to associate with this device.

   A label for the selected pool appears in the **Volume Label** field. This label will become the volume name for the device.

5. Select **Mount After Labeling** and click **OK**.

   The **Devices** window displays the device and the associated volume name.

Configuring DD Cloud Tier devices with nsradmin

Use the Device Configuration Wizard to configure NetWorker devices for the DD Cloud Tier devices.

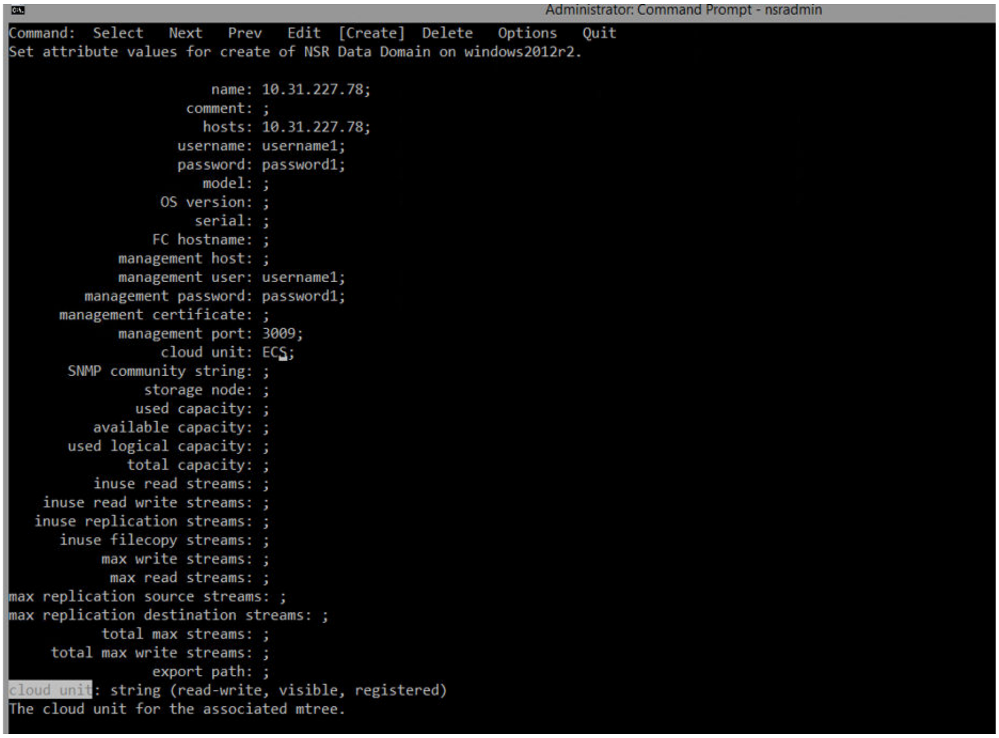
Procedure

1. Open the nsradmin tool in visual mode.

   In order to create a DD Cloud Tier device, both NSR Device and NSR Data Domain resource have to be created with certain attributes set.

2. Select the **Create** option in the menu and select the type as **NSR Data Domain**. The following screen appears with list of attributes to be configured for new data domain resource:

Figure 34 Attributes to be configured for new data domain resource



```
Command:  Select   Next   Prev   Edit  [Create]  Delete   Options   Quit
Set attribute values for create of NSR Data Domain on windows2012r2.

                        name: 10.31.227.78;
                     comment: ;
                       hosts: 10.31.227.78;
                    username: username1;
                    password: password1;
                       model: ;
                  OS version: ;
                      serial: ;
                 FC hostname: ;
             management host: ;
             management user: username1;
         management password: password1;
      management certificate: ;
             management port: 3009;
                  cloud unit: ECS;
       SNMP community string: ;
                storage node: ;
               used capacity: ;
          available capacity: ;
       used logical capacity: ;
              total capacity: ;
          inuse read streams: ;
    inuse read write streams: ;
   inuse replication streams: ;
      inuse filecopy streams: ;
           max write streams: ;
            max read streams: ;
max replication source streams: ;
max replication destination streams: ;
           total max streams: ;
     total max write streams: ;
                 export path: ;
cloud unit: string (read-write, visible, registered)
The cloud unit for the associated mtree.
```

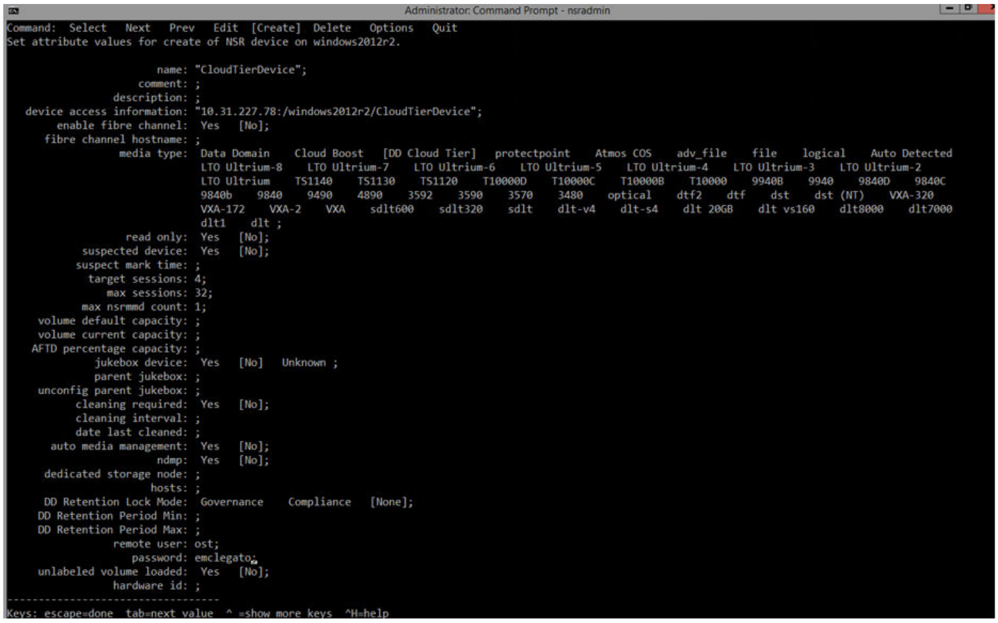
3. Set the following attributes(others are optional)

Table 4 Field and Attribute names

Field name	Attributes
Name	Data Domain system Name
username	Remote user name to connect to the Data Domain
password	Remote user password to connect to the Data Domain
Management Host	Host name of the Data Domain system
Management User	Username for a Data Domain user that has admin access. For example, sysadmin
Management Password	Specify the password of the management user
Port	Specify the management port. By default, the port is 3009
Cloud Unit Name	Specify the name of the cloud unit that you created on the Data Domain system

4. Select the **Create** option in the menu and select the type as **NSR** device. The following full screen appears with list of attributes to be configured for new device resource.

Figure 35 Attributes to be configured for new device resource



```
Command:  Select   Next   Prev   Edit  [Create]  Delete   Options   Quit
Set attribute values for create of NSR device on windows2012r2.

                        name: "CloudTierDevice";
                     comment: ;
                 description: ;
     device access information: "10.31.227.78:/windows2012r2/CloudTierDevice";
          enable fibre channel:  Yes   [No];
        fibre channel hostname: ;
                  media type:  Data Domain    Cloud Boost   [DD Cloud Tier]   protectpoint    Atmos COS    adv_file    file    logical    Auto Detected
                               LTO Ultrium-8    LTO Ultrium-7    LTO Ultrium-6    LTO Ultrium-5    LTO Ultrium-4    LTO Ultrium-3    LTO Ultrium-2
                               LTO Ultrium    TS1140    TS1130    TS1120    T10000D    T10000C    T10000B    T10000    9940B    9940    9840D    9840C
                               9840b    9840    9490    4890    3592    3590    3570    3480    optical    dtf2    dtf    dst    dst (NT)    VXA-320
                               VXA-172    VXA-2    VXA    sdlt600    sdlt320    sdlt    dlt-v4    dlt-s4    dlt 20GB    dlt vs160    dlt8000    dlt7000
                               dlt1    dlt ;
                   read only:  Yes   [No];
            suspected device:  Yes   [No];
           suspect mark time: ;
             target sessions: 4;
                max sessions: 32;
            max nsrmmd count: 1;
      volume default capacity: ;
      volume current capacity: ;
     AFTD percentage capacity: ;
              jukebox device:  Yes   [No]   Unknown ;
              parent jukebox: ;
      unconfig parent jukebox: ;
           cleaning required:  Yes   [No];
           cleaning interval: ;
           date last cleaned: ;
        auto media management:  Yes   [No];
                        ndmp:  Yes   [No];
       dedicated storage node: ;
                       hosts: ;
       DD Retention Lock Mode:  Governance    Compliance   [None];
      DD Retention Period Min: ;
      DD Retention Period Max: ;
                 remote user: ost;
                    password: emclegato;
      unlabeled volume loaded:  Yes   [No];
                 hardware id: ;
----------------------------------
Keys: escape=done  tab=next value  ^ =show more keys  ^H=help
```

5. Provide Device name, Device access information, username for the DD boost user (username filed), and password for the account (all four are mandatory attributes to create a device resource.)

   Device access information must be of the following form:

   `<DD IP>:<StorageUnitName>/<DeviceName>` where Device Name refers to the subfolder to be created within the storage unit.

   Note:

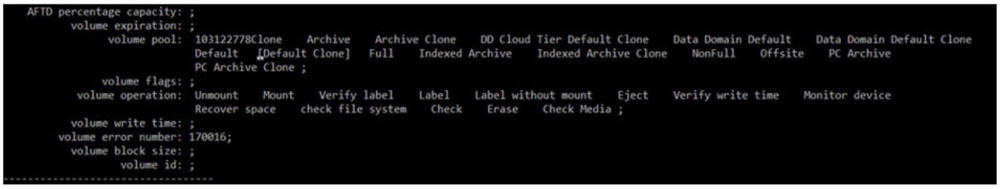
   - Device access information is parsed to get the storage unit and the device name.
   - If device with Mtree exists, then the `nsradmin` command displays the error `device already exist`.

6. Select the media type as DD Cloud Tier.
7. In order to enable the SMT feature, set the **secure multi tenancy** attribute to **Yes**. If SMT is disabled, storage unit (Mtree) name must be named after the Networker server.
8. When the attributes are set (including the optional ones), use the escape key to create the new resource. Select **Yes** to do the same, otherwise select **No**.

   Note: When you click on **Yes**, Device RAP Resource gets created along with the storage unit and device folder on the DD host. If storage node is not in ready state, `nsradmin` waits until it becomes available.

9. Click on the **Select** option which displays the types of resources available. Select the option **NSR Device**. It lists out all the devices that has been created and is available. Browse through the list using **Next** and **Previous**, once you find the device that you want to configure, click on the **Edit** option.
10. Selecting the pool in **Volume Pool** field. If you want to create a new pool, select the pool using **NSR Pool** resource and select the **Create** option. Once it is complete revert back to the current device Window (follow Step 9) and select the new pool that has just been created.

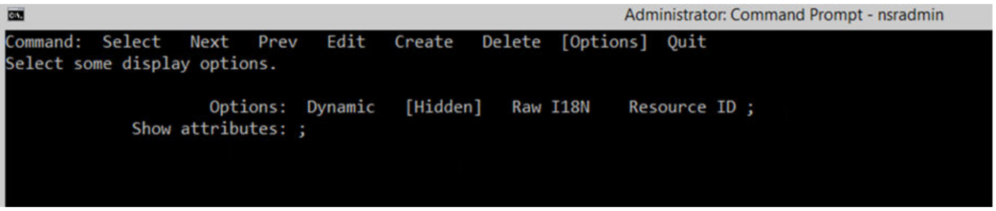
Figure 36 Configuring the media pool information



```
AFTD percentage capacity: ;
       volume expiration: ;
             volume pool: 103122778Clone    Archive    Archive Clone    DD Cloud Tier Default Clone    Data Domain Default    Data Domain Default Clone
                          Default   [Default Clone]   Full    Indexed Archive    Indexed Archive Clone    NonFull    Offsite    PC Archive
                          PC Archive Clone ;
            volume flags: ;
        volume operation: Unmount    Mount    Verify label    Label    Label without mount    Eject    Verify write time    Monitor device
                          Recover space    check file system    Check    Erase    Check Media ;
       volume write time: ;
     volume error number: 170016;
       volume block size: ;
               volume id: ;
----------------------------------
```

11. In order to configure the volume operations, enable the hidden attribute in **Options** section (If it is disabled).

    Figure 37 Enabling hidden attribute

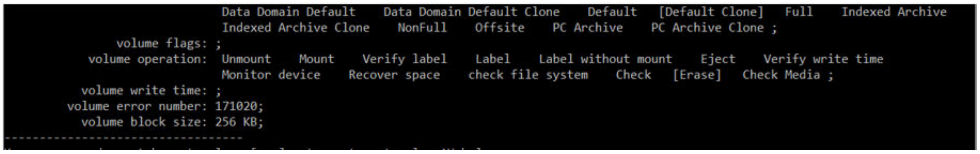
    Administrator: Command Prompt - nsradmin

    ```
    Command:  Select   Next   Prev   Edit   Create   Delete  [Options]  Quit
    Select some display options.

                   Options:  Dynamic   [Hidden]   Raw I18N    Resource ID ;
             Show attributes: ;
    ```

12. Select options available in **Volume operation** field in order to label, mount and perform other volume operations on the device. Operations have to be performed one at a time. Labeling and mounting of the device can also be performed by running the command `nsrmm -s <server_name> -v -y -m -b <pool_name> -l -f <device_name>`.
13. In order to permanently erase all data and remove media and index information erase volume operation has to be performed.

    Figure 38 Performing erase volume operation

    ```
                          Data Domain Default    Data Domain Default Clone    Default   [Default Clone]   Full    Indexed Archive
                          Indexed Archive Clone    NonFull    Offsite    PC Archive    PC Archive Clone ;
            volume flags: ;
        volume operation: Unmount    Mount    Verify label    Label    Label without mount    Eject    Verify write time
                          Monitor device    Recover space    check file system    Check   [Erase]   Check Media ;
       volume write time: ;
     volume error number: 171020;
       volume block size: 256 KB;
    ----------------------------------
    ```

14. Select **Delete** from the menu to delete the device RAP resource. Delete operation would also need device to be unmounted and removed as a target device from the corresponding NSR Pool resource.

Configuring clients to back up to DD Boost devices

You can create client resources to define backup data by using the Client Configuration wizard or manually. It is recommended that you use the Client Configuration wizard to create client resources.

Configuring a backup client with the wizard

Use the NetWorker Client Configuration wizard to create and modify NetWorker backup clients.

Before you begin

If the client is to use a Client Direct backup, which is the default configuration, ensure that the client has access to the same network connectivity (IP or FC) that the target DD Boost devices use.

Note: Mac OS X clients only support the IP protocol.

About this task

ⓘ Note: If you want to redirect existing client backups to new DD Boost devices, Redirecting backups from other devices to DD Boost provides details.
The details for the settings referred to in this simplified wizard procedure are found in the next procedure Configuring a backup client with NMC property windows.

Procedure

1. Use NMC to connect to the NetWorker server, and then click **Protection**.
2. In the left navigation pane, right-click **Clients** and select **Client Backup Configuration** > **New**.
3. Complete the fields on the following wizard pages:
   - Show the **Client Name**.
   - Specify the **Backup Configuration Type**.
   - Specify the **Backup Options**:
     - In the **Deduplication** settings, select **Data Domain Backup**, if applicable.
       This setting ensures that the client backs up only to DD Boost devices if the pool used also contains other types of devices such as AFTDs. It is best not to have mixed devices in pools.
     - Set **Target Pool** to a pool associated with DD Boost devices.
       An alternative way to configure a client to use a pool is to specify the client or its group in the **Data Source** field of the Pool resource. Creating pools to target DD Boost devices provides details.

       ⓘ Note: Current versions of NetWorker application modules support backup to DD Boost devices. Some earlier versions of modules do not support the client fields for **Data Domain backup** and **Pool**. In these cases, do not set these fields. Backup fails for older NetWorker application modules on page 180 provides details.
   - Select **Files to Back Up**.
   - Select the **Client Properties**.
   - Select the **Backup Group**.
   - Specify the **Storage Node Options**.
4. Complete the wizard.

Configuring a backup client with NMC property windows

Dell EMC recommends that you use the Client Configuration wizard to create and modify NetWorker clients. The following procedure describes how to manually create a Client resource.

Before you begin

If the client is to use a Client Direct backup, which is the default configuration, ensure that the client has access to the same network connectivity (IP or FC) that the target DD Boost devices use.

ⓘ Note: Mac OS X clients only support the IP protocol.

About this task

The *NetWorker Administration Guide* provides details on NetWorker Client resource configurations.

You can complete the following steps to configure a NetWorker client for scheduled backups to a DD Boost device.

Procedure

1. Use NMC to connect to the NetWorker server and click **Protection**.
2. In the left navigation pane, select **Clients**:
    - To create a Client resource, from the **File** menu, select **New**.
    - To edit an existing Client resource, select the client name from the list in the right panel, and from the **File** menu, select **Properties**.

    a. On the **General** tab, in the **Name** field, type the hostname for the client and, optionally, type a comment in the **Comment** field.

    b. Optional, select **Block based backup**.

    c. In the **Save Sets** field, click the **Browse** button to open the **Choose Directory** window. Browse to and select the volumes or individual file systems that you want to back up. When finished selecting, click **OK**.

    Type each item on a separate line. For example:

    ```
    E:\
    ```

    ```
    F:\
    ```

    To back up all client data, type All in the **Save Sets** field.

    ⓘ Note: For Microsoft Windows systems, back up the SYSTEM or Volume Shadow Copy Service (VSS) SYSTEM on a periodic basis to prepare for disaster recovery of the client system.
    The *NetWorker Administration Guide* provides details for this step.

3. On the **General** tab, in the **Backup** area, complete the following steps:

    a. To enable deduplicated backup data from this client to bypass the NetWorker storage node and be sent directly to the Data Domain system, select **Client Direct**. Review the following requirements:

    - Ensure that you have not selected the **Checkpoint restart** field. If selected, backups revert to traditional storage node backups.
    - Ensure that the client interface configuration, whether FC or IP, matches the DD Boost device interface configuration. If the interfaces do not match, then the storage node performs the backup and restore operations.
    - Ensure that you have configured the Data Domain system to use the DD Boost devices. Configuring the Data Domain system for DD Boost by using the CLI on page 48 provides details.
    - Ensure that you have configured the NetWorker Device resource for the Data Domain system with a **Remote User** field that specifies a DD Boost username. Configuring a DD Boost device manually on page 89 provides details.

      ⓘ Note: Client Direct access from a Linux host to a Data Domain system requires a glibc 2.3.4 or later library on the Linux system.

    b. (Optional) In the Protection group list field, select the group in which to add the Client resource. If you have not created the protection group, you can create one later and add the client to the group.

4. On the **Apps & Modules** tab, perform the following tasks:

    a. In the **Deduplication** area, select **Data Domain backup**. This ensures that NetWorker backs up the client data only to DD Boost devices, even if the selected pool contains DD Boost and other types of devices. It is best not to include different device types in a single pool.

> ⓘ Note: Current versions of NetWorker application modules support backup to DD Boost devices. Some of the earlier module versions do not support the client fields for **Data Domain backup** and **Pool**. In this case, do not set these fields. Backup fails for older NetWorker application modules on page 180 provides details.

b. In the **Data Domain Interface** field, select the type of connectivity the client uses for DD Boost devices:

- Select **IP** for TCP/IP connectivity only.
  Do not select **IP** if the **Enable fibre channel** attribute is enabled on the **Configuration** tab of the DD Boost Device resource. This conflict in settings could cause backups to fail and restores to operate only through the storage node.
- Select **Fibre Channel** for FC connectivity only.
  You cannot select the FC-only setting when you create a Client resource for the NetWorker server resource because the NetWorker server requires IP connectivity to send control information to the hosts within the datazone.
- Select **Fibre Channel** for FC connectivity only.
  You cannot select the FC-only setting when you create a Client resource for the NetWorker server resource because the NetWorker server requires IP connectivity to send control information to the hosts within the datazone.
- To enable both FC and IP connectivity to the devices, select **Any**.
  If the NetWorker server contains multiple definitions of this Client resource, any changes to this field propagate to the other instances of the client.

c. To redirect an NDMP client from a tape backup to a DD Boost backup, change the **Backup** fields as follows:

   a. Select the **NDMP** option.

   b. In the **Backup Command** field, type the following command:

```
nsrndmp -T backup_type -M
```

   where *backup_type* is dump, tar, or vbb.

   The `-M` option specifies a backup with the Data Service Agent (DSA) option.

   The *NetWorker Administration Guide* provides details on the `nsrndmp` command.

5. On the **Globals (2 of 2)** tab, in the **Configuration** area, configure the following settings:

   a. In the **Storage Nodes** field, type the hostnames of the remote storage nodes that receive the client backup data.

   b. In the **Recover Storage Nodes** field, type the hostnames of the storage nodes that you use to restore the client data.

   c. (Optional), In the **Backup target disks** field, specify an ordered list of AFTD and Data Domain disk devices that will receive data for this client. When you specify a value in this attribute, NetWorker ignores the values that you specify in the **Storage nodes** attribute. This attribute does not apply to the client resource of the NetWorker server, and applies to each instance of the client resource. You can specify devices that are local or remote to the NetWorker server.

6. When you have completed the client configuration, click **OK**.

   The NetWorker server window shows a check mark in the Scheduled backup column of clients that are enabled for scheduled backup.

Manually creating or modifying NetWorker resources for DD Boost

Dell EMC recommends that you use the Device Configuration Wizard, which is part of the NetWorker Administration GUI, to create and modify DD Boost devices. The wizard also enables you to create and modify volume labels and the storage pools for DD Boost devices.

The following section describes how to modify a DD Boost device after the wizard creates the device, how to add a Data Domain system as a managed host, and how to create or modify DD Boost pools and label templates.

Configuring DD Boost devices manually

Dell EMC recommends that you use the Device Configuration Wizard to manually add a Data Domain system to the NetWorker datazone. and create DD Boost devices. You can modify the Device resource that the wizard creates to modify the devices, and perform the tasks in the following sections.

Adding a managed Data Domain system to NMC

Procedure

1. Log in to the NMC GUI as an administrator of the NetWorker server.
2. On the taskbar, click the **Enterprise** icon.
3. In the left navigation pane:

   a. Right-click **Enterprise**.

   b. Select **New** > **Host**.

   The **Add New Host** wizard appears.
4. In the **Create Host** page:

   a. Specify the FQDN of the Data Domain system or DDVE.

   > **Note:** For a Highly Available Data Domain system, specify the floating IP or hostname of the Data Domain system.

   b. Click **Next**.
5. In the **Select Host Type** page:

   a. Select **DataDomain**.

   b. Click **Next**.
6. In the **Manage DataDomain** page:

   a. Review the configuration details.

   b. Click **Next**.

   c. Leave the **Capture Events** option selected.
7. (Optional) In the **Configure SNMP Monitoring** page, perform the following steps:

   a. In the **SNMP Community String** field, type the name of the SNMP community string.

   > **Note:** If you do not know the name of the community, leave this field blank.

b. With the **Receive SNMP trap events option selected, specify the SNMP Process** port used by the Data Domain system and select the events in which to monitor. Use the **Reset to defaults option** to reset the events in which to monitor back to the default settings.

ⓘ **Note:** The default SNMP process port is 162.

c. Click **Next**.

SNMP monitoring enables NMC to display the Data Domain system status and to list the backup and the recovery events. The monitoring feature also provides a launcher link for the Data Domain interface.

8. Click **Finish**.

Results

The Data Domain system or DDVE appears in the **Enterprise** window.

Adding a host Data Domain system to NMC Enterprise view

Use the Add New Host Wizard to manually add a Data Domain system to the NetWorker datazone.

About this task

NetWorker lists the Data Domain systems as a host in the NMC Enterprise view. This view shows the Data Domain system status and the backup and recovery events that were performed by NetWorker managed by NMC. The **Enterprise** view also provides a live link to launch the Data Domain Enterprise Manager GUI. To manually add a Data Domain system to the NMC **Enterprise** view, perform the following steps:

Procedure

1. From the **File** menu, select **New** > **Host** to run the **Add New Host** wizard.
2. Complete the wizard screens:
   - Type the Data Domain hostname.
   - Select **Data Domain**.
   - Select **Capture Events**.
   - Type the name of the SNMP community where NMC will retrieve Data Domain status information. By default, NMC uses the value configured on the Data Domain system with the `snmp add ro-community` command.
   - Type a value for the **SNMP Process Port**. By default, NMC uses the value that is configured on the Data Domain system with the `snmp add trap-hosthostname[:port]` command. This configuration must agree with the firewall configuration on the Data Domain system.
   - Select the **SNMP Traps** that you want to monitor.

Configuring a DD Boost device manually

The following procedure describes how to configure or modify the DD Boost device manually. It is recommended however for device creation that you use the NMC Device Configuration Wizard. If you manually create a DD Boost device with this procedure, NMC lists the device but does not create a corresponding device folder on the Data Domain system. If you then try to label and mount such a device, an error appears. When the device is created using the NMC Device Configuration wizard, a DD Boost device appears as a folder on the Data Domain system, and you associate each DD Boost device with a single NetWorker volume by labeling a device for a NetWorker pool.

About this task

To configure or modify a DD Boost device complete the following steps:

Procedure

1. Use NMC to connect to the NetWorker server. In the **Administration** window, click the **Devices** view.
2. In the folder tree, expand **Data Domain Systems** and select the Data Domain system that stores the save sets.
3. In the right panel, right-click the name of the device that you want to modify, and then select **Properties**.
4. On the **General** tab, identify the DD Boost device by typing its name and access information:

   ⓘ Note: Multiple devices can share a single volume. Configuring volume sharing on multiple devices provides details.

   a. In the **Name** field, type a name for the Data Domain device.

   For example:

   dd_1

   Configuring a DD Boost device manually on page 89 uses the following example values:

   - NetWorker server short hostname = *dzone1*
   - NetWorker remote storage node hostname = *dzone1_sn2*
   - Data Domain hostname = *ddr1*
   - DD Boost device name = *dd_1*

   If you configure the device on a separate storage node host that is not the NetWorker server host as shown in Configuring a DD Boost device manually on page 89, it is a remote device. Specify the **Name** field in the following format:

   rd=*remote_storagenode_hostname:device_name*

   For example:

   rd=*dzone1_sn2:dd_1*

   b. In the **Device access information** field, type the Data Domain hostname followed by a colon and the path to the device folder.

   If you are configuring a device with secure multi-tenancy (SMT) protection, the device folder must reside in a password-protected tenant unit on the Data Domain. Configuring the Data Domain system for DD Boost by using the CLI on page 48 provides details.

   Use the following format:

   DD_hostname:/ DD_storage_unit_name/ device_name

   where, as a best practice, *DD_storage_unit_name* is the short hostname of the NetWorker server and *device_name* is a name for the device, which appears as a folder.

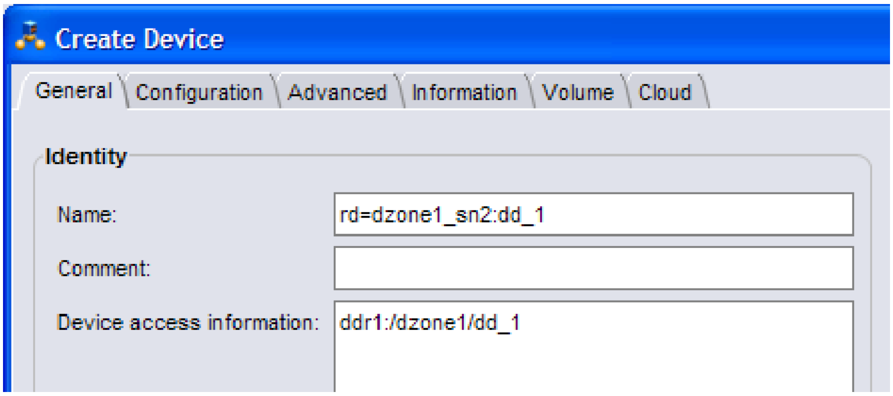
   For example, the following figure uses the following name:

   ddr1:/dzone1/dd_1

   NetWorker does not limit the number device folders that you can create, but the Device access information field accepts one device folder only. Do not create any folders within a device folder.

ⓘ **Note:** Implicit in this pathname is the hidden mount point folder `/data/col1`. Do not modify this folder structure, which all NetWorker servers use.

Figure 39 Example of the device name and the access information for a DD Boost device



Name: rd=dzone1_sn2:dd_1

Comment:

Device access information: ddr1:/dzone1/dd_1

c. In the **Media type** field, select **Data Domain** from the list.

5. On the **Configuration** tab, in the **Save Sessions** area, set the number of concurrent save sessions (streams) and the number of `nsrmmd` (media storage) processes that the device can handle:

   - In the **Target sessions** field, specify the number of save sessions that a `nsrmmd` process on the device handles before another device on the Data Domain host takes the additional sessions. If another device is not available, then another `nsrmmd` process on the same device takes the additional sessions. Use this setting to balance the sessions load among `nsrmmd` processes.

     It is recommended that you set this field to a low value. The default value is 20. The maximum value is 60.

   - In the **Max sessions** field, specify the maximum number of save sessions that the device can handle. At the maximum limit, if no additional devices are available on the host, then another available Data Domain system takes the additional sessions. If no other Data Domain hosts are available, then the system retries the save sessions until a `nsrmmd` process become available.

     The default value is 60. The maximum value is 60.

     ⓘ **Note:** The **Max sessions** setting does not apply to concurrent recovery sessions.

   - In the **Max nsrmmd count** field, specify the maximum number of `nsrmmd` processes that can run on the device. Use this setting to balance the `nsrmmd` load among devices.

     If you enabled **Dynamic nsrmmds** on the storage node, NetWorker automatically adjusts this value by using the formula max/target +4, with the default value being 14. Otherwise, the default value is 4.

     To modify this value, first adjust the two sessions fields, apply and monitor the effects, and then tweak the **Max nsrmmd count** value.

     ⓘ **Note:** NetWorker reserves at least one `nsrmmd` process for restore and clone operations.

6. In the **Remote user** and **Password** fields, type the DD Boost username and password, respectively.

   You can only define one DD Boost (OST) user. All NetWorker storage nodes and servers that access the Data Domain system must use the same username and password.

> **Note:** Avoid changing the user of an existing device with a labeled volume. The new user will not have write permission to the files and directories that are created by the previous user and cannot re-label the volume. Create a device for the new user.

7. If you want the DD Boost device to use FC connectivity, complete the following steps:

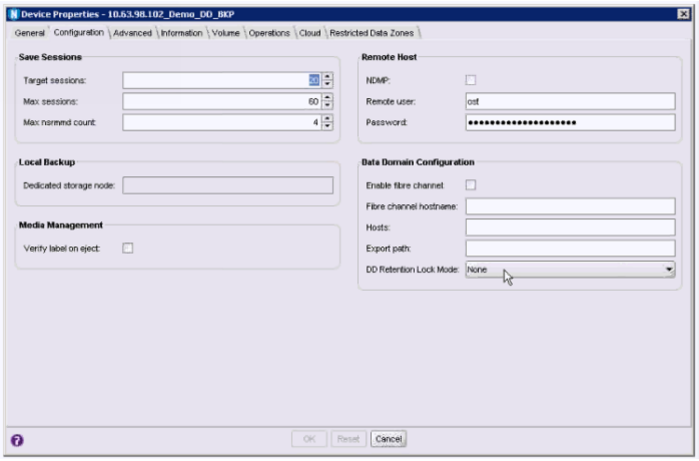
   a. Select the **Enable fibre channel** field.

   b. In the **Fibre Channel Host Name** field, type the hostname that the Data Domain system uses to identify itself for FC operations. By default, this hostname is the same name used for IP operations, but the hostnames can be different. The hostname must match the Server Name displayed on the Data Domain system in the **Data Management** > **DD Boost** > **Fibre Channel** tab of the **Data Domain Enterprise Manager**. The name is case-sensitive.

   > **Note:** All NetWorker clients that use an FC-enabled DD Boost device must be enabled for FC in the **Data Domain Interface** field.

8. If you want to enable DD Retention Lock on the Data Domain device, select **Governance mode** or **Compliance mode** from the DD Retention Lock Mode drop-down. If you do not want to use DD Retention Lock on this device, select **None**.

Figure 40 Data Domain Device Properties Configuration tab



Device Properties - 10.63.98.102_Demo_DD_BKP

Save Sessions

Target sessions: 20

Max sessions: 60

Max nsrmmd count: 4

Remote Host

NDMP: □

Remote user: ost

Password: ••••••••••••••••••••

Local Backup

Dedicated storage node:

Media Management

Verify label on eject: □

Data Domain Configuration

Enable fibre channel: □

Fibre channel hostname:

Hosts:

Export path:

DD Retention Lock Mode: None

9. If you want to enable **Compliance mode** on the device, manually enable compliance mode on the device Mtree before enabling it on the NetWorker device.

10. To save the device settings click **OK**.

    The NetWorker **Administration** window displays the Data Domain system and details of the device.

11. Ensure that the device is associated with a NetWorker storage volume before you try to use the device. Otherwise, an error appears. Labeling and mounting devices on the storage node provides the procedure.

Configuring volume sharing on multiple devices

You can concurrently mount and share a single NetWorker storage volume with multiple DD Boost devices, to provide greater flexibility and performance gains.

- A volume that you simultaneously mounted on both an IP-enabled DD Boost device and an FC-enabled DD Boost device provides greater flexibility. Clients, including Client Direct clients, can back up and restore their data on the same volume over either IP or FC networks. Restoring by

Client Direct over IP from an FC-enabled device provides details on a volume sharing solution for restore operations.

- You can create multiple devices for shared volumes on the same storage node or on separate storage nodes.
- For clients that are not Client Direct clients, a shared volume can improve bandwidth for backup or restore operations to a DD Boost device because NetWorker can use the storage node that is closest to the requesting client.

  ⓘ Note: In some environments however, concurrent read or write operations to a volume from multiple storage nodes or Client Direct clients can result in disk thrashing that impairs performance.

You must create each device separately, with a different name, and you must correctly specify the path to the storage volume location.

For example, to create three devices, one on the NetWorker server host named dzone1 that uses local devices and two remote devices (rd) on storage nodes dzone1_sb2 and dzone1_sn3, specify the name of each device in **Name** field of each device as follows:

```
dd_1a

rd=dzone1_sn2:dd_1b

rd=dzone1_sn3:dd_1c
```

The **Device access information** field would specify the same single directory as a valid complete path for each alias.

For example, for a directory named dd_1 on the Data Domain storage host named ddr1, specify the correct pathname:

- If the storage node uses an automounter, you can specify the following pathname:

  ```
  /net/ddr1/dzone1/dd_1
  ```

- If the storage node uses an explicit system mount point, you can specify one of the following pathnames:

  ```
  /mnt/ddr1/dzone1/dd_1

  /mnt/dzone1/dd_1
  ```

Creating a volume label template for DD Boost devices

When you use the Device Configuration Wizard, the wizard automatically creates a label template for the volumes that a new device will use.

About this task

ⓘ Note: The Device Configuration Wizard automatically creates a label template for the volumes, and this procedure does not apply if you use the wizard.

Each DD Boost device is associated with a single volume. The label template that is assigned to the pool determines the volume name. NetWorker mounts each volume in a DD Boost device. A label template provides a DD Boost device with a volume name and numbering to all storage volumes that belong to the same pool.

A label template defines the components of a volume label, which includes the volume name, a separator, and volume number. All the volumes in the same pool will have the same label name, for example, dd_myvol, but different volume numbers, for example, .001.003.

For example, a Data Domain system may have three devices, each of which is mounted with a storage volume (Volume Name). If each device/volume is associated with the same pool, the volume names would be as follows:

- dd_myvol.001
- dd_myvol.002
- dd_myvol.003

To create a label template, perform the following steps:

Procedure

1. In the **NetWorker Administration** window, click **Media**.
2. In the browser tree, select **Label Templates**, and from the **File** menu, click **New**.

   The **Create Label Template** window appears.
3. In the **Name** and **Comment** fields, type a name and description for the label template. The label will associate a storage pool to a device.
4. In the **Fields** field, type the components of the label. Place each label component on a separate line. The template must include at least one volume number range component. NetWorker applies the label template to the volumes mounted on DD Boost devices in a Data Domain system.

   For example:

   dd_myvol

   001-999
5. Select a **Separator**, and click **OK**.
6. In the **Next** field, specify the next volume label in the sequence to be applied during the next label and mount operation, for example, dd_myvol.001.
7. Click **OK**.

Creating pools to target DD Boost devices

Typically, use the Device Configuration Wizard, which automatically creates a media pool. The following procedure describes the alternative manual method that uses the NMC property windows.

About this task

Each NetWorker client stores data to a media or target pool. This pool is used to direct the data from backup clients, or the data from storage volumes for clone operations, to the storage devices that are members of the pool.

Each DD Boost device is associated with a storage volume label when it is mounted. The Volume Name value of the storage volume implicitly associates the device with the specified pool.

ⓘ **Note:** Dynamic Drive sharing (DDS) is not supported for DD Boost devices.

Complete the following steps to manually create a pool for Data Domain backups:

Procedure

1. Ensure that the devices that you assign to the pool were created in NetWorker.
2. Ensure that a label template has been created for the pool. Creating a volume label template for DD Boost devices on page 93 provides details.
3. From the **NetWorker Administration** window, click **Media**.
4. In the left navigation pane, select **Media Pools**, and from the **File** menu, select **New** to open the **Create Media Pool** window with the **Basic** tab selected.
5. In the **Name** field, type a name for each pool. Create names that clearly indicate whether the pool is for a Data Domain backup or a Data Domain clone operation.

For example:

DDsite1

DDCLsite2

A pool name that starts with DD would be a Data Domain pool, and a pool name that starts with DDCL would be a Data Domain clone pool. The pool name can also include the physical location where NetWorker stores the backup data. These conventions make the name easier to use for scripting and reporting.

6. (Optional) In the **Comment** field, type a description of the pool.
7. Select **Enabled**.
8. Select the **Pool type**:
   - To use the pool for backups, select **Backup**.
   - To use the pool for clone copies, select **Backup Clone**.

     Note: You cannot modify the **Pool type** value after you create the device.
9. In the **Label Template** field, select a label template to associate with the pool.

   You can later apply the pool to DD Boost devices. Labeling and mounting devices on the Data Domain device on page 96 provides details.
10. On the **Selection Criteria** tab, under **Target Devices,** select all the DD Boost devices that this pool may use for storage. The pool may store data on any of these devices. Use the following practices:
    - Select only DD Boost devices for the pool. Do not mix DD Boost devices with other types of storage devices. If you modify a pool in this step, ensure that the pool excludes all devices that are not DD Boost devices.
    - Select only DD Boost devices that reside on the same Data Domain system. To add DD Boost devices that reside on other Data Domain systems, first save the pool configuration, and then modify the pool and add the DD Boost devices.
    - Do not select devices that reside on more than one Data Domain system. Backups from a single NetWorker client can target any of these Data Domain systems. This behavior impairs the backup window and deduplication ratio.

    Note: Backups from a single NetWorker client can target any of these Data Domain systems. This behavior impairs the backup window and deduplication ratio.
11. Under **Media type required**, if you intend to use the pool for a Data Domain backup only, set this field to **Data Domain**. This setting ensures that only Data Domain devices use this pool.

    Note: It is recommended that you do not include different media types in a single pool. Backup fails for older NetWorker application modules on page 180 provides further details.
12. Click **OK**.

    The *NetWorker Administration Guide* provides details on media pools.

Labeling and mounting devices on the Data Domain device

Dell EMC recommends that you use the Device Configuration Wizard to create a Data Domain device, which automatically labels and mounts the device. The following procedure describes the alternative manual method that uses the NMC property windows.

About this task

Before you can use a device you must label and mount the device.

Procedure

1. In the **NetWorker Administration** window, click **Devices**.
2. In the left navigation pane, select **Data Domain Systems**.
3. In the right panel, right-click the device you want to label and select **Label**.
4. In the **Label** window and **Pools** list box, select a pool to associate with the device.

   A label for the selected pool appears in the **Volume Label** field. This label will become the volume name for the device.
5. Select **Mount After Labeling** and click **OK**.

   The **Devices** window displays the device and the associated volume name.

Deactivating and removing DD Boost devices

To prevent NetWorker from using the DD Boost device, you can convert the DD Boost device to read-only, disable the device, or delete the device.

Converting a device to read-only

When you convert a DD Boost device to read-only mode, NetWorker cannot use of the device for backup operations. You can continue to use the device for read operations (for example, restore operations) and as the read device for clone operations.

Procedure

1. Use NMC to connect to the NetWorker server, and select the **Devices** view. In the navigation pane, select the **Data Domain Systems** folder.
2. In the **Devices** table, right-click the device that you want to convert to read-only, and select **Unmount**.
3. Right-click this unmounted device, and select **Modify Device Properties**.
4. On the **General** tab, select **Read Only**, and click **OK**.
5. Right-click the device, and select **Mount**.

Disabling a device

When you disable a DD Boost device, NetWorker does not use the device for backup, recovery, or clone operations. You can reenable the device to restore old data that is retained on the device.

Procedure

1. Use NMC to connect to the NetWorker server, select the **Devices** view. In the left navigation pane, select the **Data Domain Systems** folder.
2. In the **Data Domain Systems** table, right-click the device that you want to disable, and select **Unmount**.

3. Right-click the device, and select **Enable/Disable**.
4. Confirm that the **Enabled** column of the table contains **No**, which indicates that you have disabled the device.

Deleting an AFTD or a DD Boost device

When you delete an AFTD or a DD Boost device you can erase the data on the volume, denoted by the access path, that stores the device's data. You can erase the volume only if no other device in the system shares the volume.

Procedure

1. Use NetWorker Management Console (NMC) to connect to the NetWorker server, and select the **Devices** view. In the left navigation pane, click **Device**.
2. In the **Devices** table, right-click the device that you want to remove, and then select **Delete**.

   A confirmation window appears.

3. Specify whether you want to erase the data on the device.
   - To delete the device without erasing the data on the device, click **Yes**.
   - To delete the device and erase the data on the device and the volume access path, select **Permanently erase all data and remove media and index information for any selected AFTDs or Data Domain devices**, and then click **Yes**.

     ⓘ Note: If another device shares the volume that you want to erase, then an error message displays the name of the other device. Before you can erase the volume, you must delete all other devices that share the volume until the last one remaining.
4. If you did not unmount the device or did not remove the device from all the Pool resource configurations, then a confirmation window appears, which provides these details. To confirm the device unmount, the removal of the device from the pool, and the deletion of the device, click **Yes**.

CHAPTER 4

Data Protection Policies

This chapter includes the following topics:

Performing clone and replicate operations

Data Protection policies provide you with the ability to backup data, which you can then clone and replicate.

Overview of protection policies

A protection policy allows you to design a protection solution for your environment at the data level instead of at the host level. With a data protection policy, each client in the environment is a backup object and not simply a host.

Data protection policies enable you to back up and manage data in a variety of environments, as well as to perform system maintenance tasks on the NetWorker server. You can use either the **NetWorker Management Web UI** or the NMC **NetWorker Administration** window to create your data protection policy solution.

A data protection policy solution encompasses the configuration of the following key NetWorker resources:

Policies

Policies provide you with a service-catalog approach to the configuration of a NetWorker datazone. Policies enable you to manage all data protection tasks and the data protection lifecycle from a central location.

Policies provide an organizational container for the workflows, actions, and groups that support and define the backup, clone, management, and system maintenance actions that you want to perform.

Workflows

The policy workflow defines a list of actions to perform sequentially or concurrently, a schedule window during which the workflow can run, and the protection group to which the workflow applies. You can create a workflow when you create a new policy, or you can create a workflow for an existing policy.

A workflow can be as simple as a single action that applies to a finite list of Client resources, or a complex chain of actions that apply to a dynamically changing list of resources. In a workflow, some actions can be set to occur sequentially, and others can occur concurrently.

You can create multiple workflows in a single policy. However, each workflow can belong to only one policy. When you add multiple workflows to the same policy, you can logically group data protection activities with similar service level provisions together, to provide easier configuration, access, and task execution.

Protection groups

Protection groups define a set of static or dynamic Client resources or save sets to which a workflow applies. There are also dedicated protection groups for backups in a VMware environment or for snapshot backups on a NAS device. Review the following information about protection groups:

- Create one protection group for each workflow. Each group can be assigned to only one workflow.
- You can add the same Client resources and save sets to more than one group at a time.
- You can create the group before you create the workflow, or you can create the group after you create the workflow and then assign the group to the workflow later.

Actions

Actions are the key resources in a workflow for a data protection policy and define a specific task (for example, a backup or clone) that occurs on the client resources in the group assigned to the workflow. NetWorker uses a work list to define the task. A work list is composed of one or several work items. Work items include client resources, virtual machines, save sets, or tags. You can chain multiple actions together to occur sequentially or concurrently in a workflow. All chained actions use the same work list.

When you configure an action, you define the days on which to perform the action, as well as other settings specific to the action. For example, you can specify a destination pool, a retention period, and a target storage node for the backup action, which can differ from the subsequent action that clones the data.

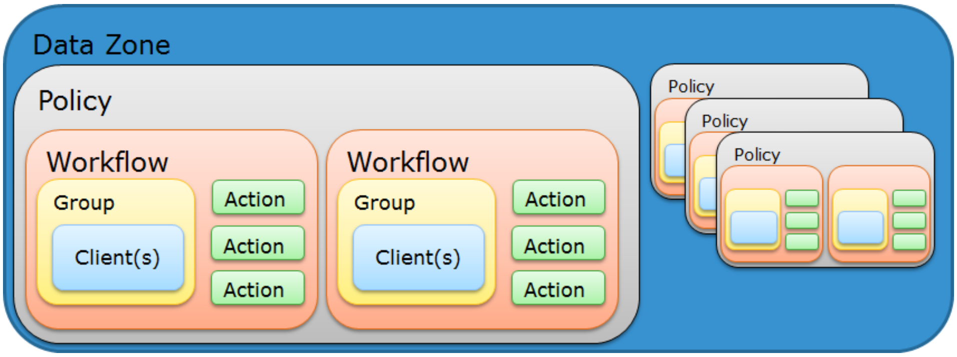
When you create an action for a policy that is associated with the virtual machine backup, you can select one of the following data protection action types:

- Backup — Performs a backup of virtual machines in vCenter to a Data Domain system. You can only perform one VMware backup action per workflow. The VMware backup action must occur before clone actions.
- Clone — Performs a clone of the VMware backup on a Data Domain system to any clone device that NetWorker supports (including Data Domain system or tape targets). You can specify multiple clone actions. Clone actions must occur after the Backup action.

You can create multiple actions for a single workflow. However, each action applies to a single workflow and policy.

The following figure provides a high level overview of the components that make up a data protection policy in a datazone.

Figure 41 Data Protection Policy



Default data protection policies in NMC's NetWorker Administration window

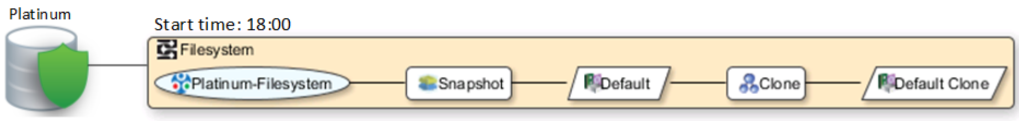
The NMC **NetWorker Administration** window provides you with pre-configured data protection policies that you can use immediately to protect the environment, modify to suit the environment, or use as an example to create resources and configurations. To use these pre-configured data protection policies, you must add clients to the appropriate group resource.

Note: NMC also includes a pre-configured Server Protection policy to protect the NetWorker and NMC server databases.

Platinum policy

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

Figure 42 Platinum policy configuration



Gold policy

The Gold policy provides an example of a data protection policy for an environment that contains virtual machines and requires backup data redundancy.

Silver policy

The Silver policy provides an example of a data protection policy for an environment that contains machines where file systems or applications are running and requires backup data redundancy.

Bronze policy

The Bronze policy provides an example of a data protection policy for an environment that contains machines where file systems or applications are running.

Strategies for traditional backups

The primary considerations for a traditional backup strategy are the groups of Client resources, the workflows that define the series of actions that are associated with the backup, and the schedule for the backup.

Overview of configuring a new data protection policy

About this task

The following steps are an overview of the tasks to complete, to create and configure a data protection policy.

Procedure

1. Create a policy resource.

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

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

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

3. Create a protection group resource.

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

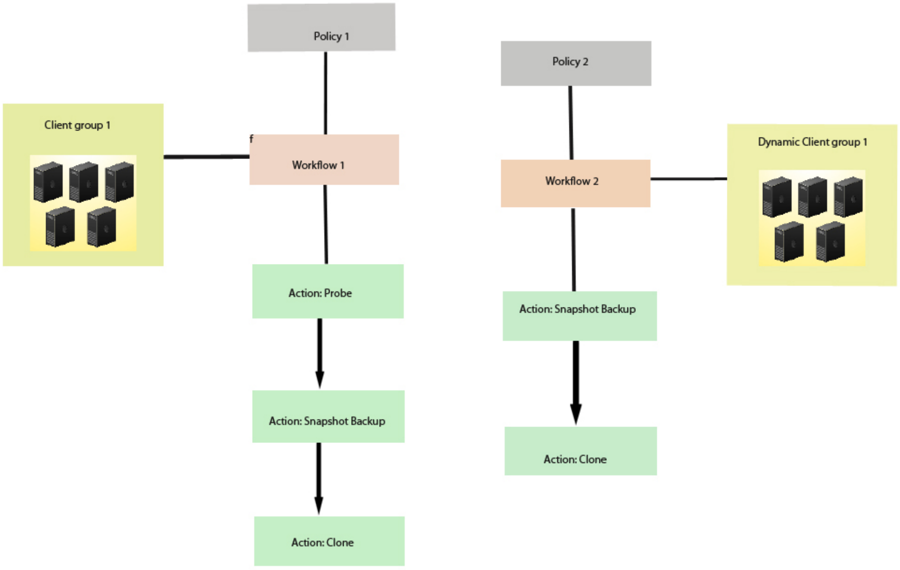
4. Create one or more action resources for the workflow resource.

5. Configure client resources, to define the backup data that you want to protect, and then assign the client resources to a protection group.

Example 1 Example of a data protection policy with 2 workflows

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

Figure 43 Data protection policy example



ⓘ **Note:** For more information on configuring a new data protection policy using the NetWorker Management Web UI, see the *NetWorker Administration Guide*.

Creating a policy

Procedure

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

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

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

   - Legal Characters: _ : - + = # , . % @
   - Illegal Characters: /*?[]()$!^;'"`~><&|{}

   ⓘ **Note:** After you create a policy, the **Name** attribute is read-only.

4. In the **Comment** field, type a description for the policy.
5. From the **Send Notifications** list, select whether to send notifications for the policy:
    - To avoid sending notifications, select **Never**.
    - To send notifications with information about each successful and failed workflow and action, after the policy completes all the actions, select **On Completion**.
    - To send a notification with information about each failed workflow and action, after the policy completes all the actions, select **On Failure**.
6. In the **Send notification** attribute, when you select the **On Completion** option or **On failure** option, the **Command** box appears. Use this box to configure how NetWorker sends the notifications. You can use the `nsrlog` command to send the notifications to a log file or you can send an email notification.

    The default notification action is to send the information to the `policy_notifications.log` file. By default, the `policy_notifications.log` file is located in the `/nsr/logs` directory on Linux and in the `C:\Program Files\EMC NetWorker\nsr\logs` folder on Windows.

    To send email messages or the `smtpmail` application on Windows, use the default mailer program on Linux:

    - To send notifications to a file, type the following command, where `policy_notifications.log` is the name of the file:

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

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

      ```
      mail -s subject recipient
      ```

    - For NetWorker Virtual Edition (NVE), to send an email notification, type the following command:

      ```
      /usr/sbin/sendmail -v recipient_email "subject_text"
      ```

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

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

      where:

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

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

After you finish

Create the workflows and actions for the policy.

Create a workflow for a new policy in NetWorker Administration

Procedure

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

   The maximum number of allowed characters for the **Name** field is 64.

   - Legal Characters: _ : - + = # , . % @
   - Illegal Characters: /*?[]()$!^;'"`~><&|{}

5. In the **Comment** box, type a description for the workflow.

   The maximum number of allowed characters for the **Comment** field is 128.

6. From the **Send Notifications** list, select how to send notifications for the workflow:

   - To use the notification configuration that is defined in the policy resource to specify when to send a notification, select **Set at policy level**.
   - To send notifications with information about each successful and failed workflow and action, after the workflow completes all the actions, select **On Completion**.
   - To send notifications with information about each failed workflow and action, after the workflow completes all the actions, select **On Failure**.

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

   The default notification action is to send the information to the `policy_notifications.log` file. By default, the `policy_notifications.log` file is located in the `/nsr/logs` directory on Linux and in the `C:\Program Files\EMC NetWorker\nsr\logs` folder on Windows.

   Use the default mailer program on Linux to send email messages, or use the `smtpmail` application on Windows:

   - To send notifications to a file, type the following command, where `policy_notifications.log` is the name of the file:

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

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

     ```
     mail -s subject recipient
     ```

   - For NetWorker Virtual Edition (NVE), to send an email notification, type the following command:

     ```
     /usr/sbin/sendmail -v recipient_email "subject_text"
     ```

   - On Windows, type the following command:

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

   where:

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

8. In the **Running** section, perform the following steps to specify when and how often the workflow runs:

   a. To ensure that the actions that are contained in the workflow run when the policy or workflow starts, in the **Enabled** box, leave the option selected. To prevent the actions in the workflow from running when the policy or workflow that contains the action starts, clear this option.

   b. To start the workflow at the time that is specified in the **Start time** attribute, on the days that are defined in the action resource, in the **AutoStart Enabled** box, leave the option selected. To prevent the workflow from starting at the time that is specified in the **Start time** attribute, clear this option.

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

      The default value is 9:00 PM.

   d. To specify how frequently to run the actions that are defined in the workflow over a 24-hour period, use the **Interval** attribute spin boxes. If you are performing transaction log backup as part of application-consistent protection, you must specify a value for this attribute in order for incremental transaction log backup of SQL databases to occur.

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

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

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

      For example, if the **Start Time** is 7:00 PM, the **Interval** is 1 hour, and the **Interval End** is 11:00 PM., then the workflow automatically starts every hour beginning at 7:00 PM. and the last start time is 11:00 PM.

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

After you finish

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

Protection groups for traditional backups

A protection groups for traditional backups identifies the client resources to back up.

Traditional backups support the following types of protection groups:

- Basic client group—A static list of client resources to back up.

- Dynamic client group—A dynamic list of client resources to back up. A dynamic client group automatically generates a list of the client resources that use a client tag which matches the client tag that is specified for the group.

Create multiple groups to perform different types of backups for different Client resources, or to perform backups on different schedules. For example:

- Create one group for backups of clients in the Accounting department, and another group for backups of clients in the Marketing department.
- Create one group for file system backups and one group for backups of Microsoft Exchange data with the NetWorker Module for Microsoft.
- Create one group for a workflow with backups actions that start at 11 p.m., and another group for a workflow with backup actions that start at 2 a.m.

Note: A Client resource can belong to more than one group.

Creating a basic client group

Use basic client groups to specify a static list of client resources for a traditional backup, a check connectivity action, or a probe action.

Before you begin

Create the policy and workflow resources in which to add the protection group to.

Procedure

1. In the **NetWorker Administration** window, click **Protection**.
2. In the expanded left pane, right-click **Groups** and select **New** from the drop-down, or right-click an existing group and select **Edit** from the drop-down.

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

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

   - Legal Characters: _ : - + = # , . % @
   - Illegal Characters: /*?[]()$!^;'"`~><&|{}

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

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

After you finish

Create Client resources. Assign clients to a protection group, by using the Client Configuration wizard or the **General** tab on the **Client Properties** page.

Creating a dynamic client group

Dynamic client groups automatically include group settings when you add client resources to the NetWorker datazone. You can configure a dynamic group to include all the clients on the

NetWorker server or you can configure the dynamic client group to perform a query that generates a list of clients that is based on a matching tag value.

About this task

A tag is a string attribute that you define in a Client resource. When an action starts in a workflow that is a member of a tagged dynamic protection group, the policy engine dynamically generates a list of client resources that match the tag value.

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

Procedure

1. In the **NetWorker Administration** window, click **Protection**.
2. In the expanded left pane, right-click **Groups** and select **New** from the drop-down, or right-click an existing group and select **Edit** from the drop-down.

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

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

   - Legal Characters: _ : - + = # , . % @
   - Illegal Characters: /*?[]()$!^;'"`~><&|{}

   Note: After you create a group, the **Name** attribute is read-only.
4. From the **Group Type** list, select **Dynamic Clients**. For steps 5 to 8, follow the instructions given in Creating a client group.

Supported actions in traditional backup workflows

Traditional backup workflows can optionally include a probe or check connectivity action before the backup, and a clone action either concurrently with or after the backup.

Probe

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

Only a backup action can follow a probe action.

Note: In-built commands from NetWorker should be avoided as probe command.

Check connectivity

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

Traditional backup

A traditional backup is a scheduled backup of the save sets defined for the Client resources in the assigned group. You must specify the destination storage node, destination pool, the schedule (period and activity), and the retention period for the backup.

Clone

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

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

Note: The clone action clones the scheduled backup save sets only, and it does not clone the manual backup save sets. Some NetWorker module backups might appear to be scheduled backups that are initiated by a policy backup action, but they are manual backups because they are initiated or converted by a database or application. The *NetWorker Module for Databases and Applications Administration Guide* and the *NetWorker Module for SAP Administration Guide* provides more details.

Actions sequences in traditional backup workflows

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

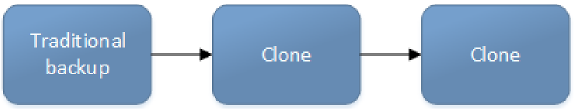
A workflow for a traditional backup can optionally include a probe or check connectivity action before the backup, and a clone action either concurrently with or after the backup.

The following supported actions can follow the lead action and other actions in a workflow.

Workflow path from a traditional backup action

The only action that can follow a traditional backup is a clone action.

Figure 44 Workflow path from a traditional backup action



Creating a check connectivity action

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

Before you begin

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

Procedure

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

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

    The **Policy Action** wizard opens on the **Specify the Action Information** page.

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

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

    - Legal Characters: _ : - + = # , . % @
    - Illegal Characters: /*?[]()$!^;'"`~><&|{}

3. In the **Comment** field, type a description for the action.

4. To ensure that the action runs when the policy or workflow that contains the action is started, in the **Enabled** box, select the option. To prevent the action from running when the policy or workflow that contains the action is started, clear this option.

   Note: When you clear the **Enabled** option, actions that occurs after a disabled action do not start, even if the subsequent options are enabled.

5. From the **Action Type** list, select **Check Connectivity**.
6. If you create the action as part of the workflow configuration, the workflow appears automatically in the **Workflow** box and the box is dimmed.
7. Specify the order of the action in relation to other actions in the workflow:
   - If the action is part of a sequence of actions in a workflow path, in the **Previous** box, select the action that should precede this action.
   - If the action should run concurrently with an action, in the **Previous** box, select the concurrent action, and then select the **Concurrent** checkbox.
8. Specify a weekly, monthly, or reference schedule for the action:
   - To specify a schedule for each day of the week, select **Define** option under **Select Schedule** and period as **Weekly by day**.
   - To specify a schedule for each day of the month, select **Define** option under **Select Schedule** and period as **Monthly by day**.
   - To specify a customized schedule to the action, select **Select** option under **Select Schedule** and choose a customized schedule using the drop down menu that is already created under NSR schedule resource.
9. Specify the days to check connectivity with the client:
   - To check connectivity on a specific day, click the **Execute** icon on the day.
   - To skip a connectivity check on a specific day, click the **Skip** icon on the day.
   - To check connectivity every day, select **Execute** from the list, and then click **Make All**.

   The following table provides details about the icons.

Table 5 Schedule icons

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

10. Click **Next**.

    The **Specify the Connectivity Options** page appears.
11. Select the success criteria for the action:
    - To specify that the connectivity check is successful only if the connectivity test is successful for all clients in the assigned group, select the **Succeed only after all clients succeed** checkbox.
    - To specify that the connectivity check is successful if the connectivity test is successful for one or more clients in the assigned group, clear the checkbox.
12. Click **Next**.

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

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

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

14. In the **Parallelism** field, specify the maximum number of concurrent operations for the action. This is applicable if multiple rollover is implemented at an action level.

15. From the **Failure Impact** list, specify what to do when a job fails:

    - To continue the workflow when there are job failures, select **Continue**.
    - To abort the current action if there is a failure with one of the jobs, but continue with subsequent actions in the workflow, select **Abort action**.

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

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

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

17. From the **Hard Limit** list, select the amount of time after the action starts to begin terminating activities. The default value of 0 (zero) indicates no amount of time.

18. (Optional) In **Start Time** specify the time to start the action.

    Use the spin boxes to set the hour and minute values, and select one of the following options from the drop-down list:

    - **Disabled**—Do not enforce an action start time. The action will start at the time defined by the workflow.
    - **Absolute**—Start the action at the time specified by the values in the spin boxes.
    - **Relative**—Start the action after the period of time defined in the spin boxes has elapsed after the start of the workflow.

19. (Optional) Configure overrides for the task that is scheduled on a specific day.

    To specify the month, use the navigation buttons and the month list box. To specify the year, use the spin boxes. You can set an override in the following ways:

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

      ⓘ Note:

      - ▪ You can edit or add the rules in the **Override** field.
      - ▪ To remove an override, delete the entry from the **Override** field.
      - ▪ If a schedule is associated to an action, then override option is disabled.

20. Click **Next**.

    The **Action Configuration Summary** page appears.

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

After you finish

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

- Probe
- Traditional backup

  Note: This option is not available for NAS snapshot backups.

- Snapshot backup

Creating a probe action

A probe action runs a user-defined script on a NetWorker client before the start of a backup. A user-defined script is any program that passes a return code. If the return code is 0 (zero), then a client backup is required. If the return code is 1, then a client backup is not required. In-built commands from NetWorker should be avoided as probe command.

Before you begin

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

Procedure

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

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

    The **Policy Action** wizard opens on the **Specify the Action Information** page.

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

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

    - Legal Characters: _ : - + = # , . % @
    - Illegal Characters: /*?[]()$!^;'"`~><&|{}

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

    Note: When you clear the **Enabled** option, actions that occurs after a disabled action do not start, even if the subsequent options are enabled.

5. From the **Action Type** list, select **Probe**.

6. If you create the action as part of the workflow configuration, the workflow appears automatically in the **Workflow** box and the box is dimmed.
7. Specify the order of the action in relation to other actions in the workflow:
   - If the action is part of a sequence of actions in a workflow path, in the **Previous** box, select the action that should precede this action.
   - If the action should run concurrently with an action, in the **Previous** box, select the concurrent action, and then select the **Concurrent** checkbox.
8. Specify a weekly, monthly, or reference schedule for the action:
   - To specify a schedule for each day of the week, select **Define** option under **Select Schedule** and period as **Weekly by day**.
   - To specify a schedule for each day of the month, select **Define** option under **Select Schedule** and period as **Monthly by day**.
   - To specify a customized schedule to the action, select **Select** option under **Select Schedule** and choose a customized schedule using the drop down menu that is already created under NSR schedule resource.
9. Specify the days to probe the client:
   - To perform a probe action on a specific day, click the **Execute** icon on the day.
   - To skip a probe action, click the **Skip** icon on the day.
   - To perform a probe action every day, select **Execute** from the list, and then click **Make All**.

   The following table provides details on the icons.

   Table 6 Schedule icons

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

10. Click **Next**.

    The **Specify the Probe Options** page appears.
11. Specify when to start the subsequent backup action:
    - To start the backup action only if all the probes associated with client resources in the assigned group succeed, select the **Start backup only after all probes succeed** checkbox
    - To start the backup action if any of the probes associated with a client resource in the assigned group succeed, clear the **Start backup only after all probes succeed** checkbox.
12. Click **Next**.

    The **Specify the Advanced Options** page appears.
13. In the **Retries** field, specify the number of times that NetWorker should retry a failed probe or backup action, before NetWorker considers the action as failed. When the **Retries** value is 0, NetWorker does not retry a failed probe or backup action.

ⓘ Note: The **Retries** option applies to probe actions, and the backup actions for the Traditional and Snapshot action types. If you specify a value for this option for other actions, NetWorker ignores the values.

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

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

15. In the **Inactivity Timeout** field, specify the maximum number of minutes that a job run by an action can try to respond to the server.

    If the job does not respond within the specified time, the server considers the job a failure and NetWorker retries the job immediately to ensures that no time is lost due to failures.

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

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

16. In the **Parallelism** field, specify the maximum number of concurrent operations for the action. This is applicable if multiple rollover is implemented at an action level.
17. From the **Failure Impact** list, specify what to do when a job fails:
    - To continue the workflow when there are job failures, select **Continue**.
    - To abort the current action if there is a failure with one of the jobs, but continue with subsequent actions in the workflow, select **Abort action**.

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

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

18. Do not change the default selections for the Notification group box. NetWorker does not support notifications for probe actions and ignores and specified values.
19. From the **Soft Limit** list, select the amount of time after the action starts to stop the initiation of new activities. The default value of 0 (zero) indicates no amount of time.
20. From the **Hard Limit** list, select the amount of time after the action starts to begin terminating activities. The default value of 0 (zero) indicates no amount of time.
21. (Optional) In **Start Time** specify the time to start the action.

    Use the spin boxes to set the hour and minute values, and select one of the following options from the drop-down list:
    - **Disabled**—Do not enforce an action start time. The action will start at the time defined by the workflow.
    - **Absolute**—Start the action at the time specified by the values in the spin boxes.

- **Relative**—Start the action after the period of time defined in the spin boxes has elapsed after the start of the workflow.

22. (Optional) Configure overrides for the task that is scheduled on a specific day.

    To specify the month, use the navigation buttons and the month list box. To specify the year, use the spin boxes. You can set an override in the following ways:

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

    > **Note:**
    >
    > - You can edit or add the rules in the **Override** field.
    > - To remove an override, delete the entry from the **Override** field.
    > - If a schedule is associated to an action, then override option is disabled.

23. Click **Next**.

    The **Action Configuration Summary** page appears.

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

Creating a traditional backup action

A traditional backup is a scheduled backup of the save sets defined for the Client resources in the assigned group for the workflow.

Before you begin

- Create the policy and workflow that contain the action.
- Optional, create actions to precede the backup action in the workflow. Supported actions that can precede a backup include:
    - Probe
    - Check connectivity

Procedure

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

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

    The **Policy Action** wizard opens on the **Specify the Action Information** page.

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

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

    - Legal Characters: _ : - + = # , . % @
    - Illegal Characters: /*?[]()$!^;'"`~><&|{}

3. In the **Comment** field, type a description for the action.

4. To ensure that the action runs when the policy or workflow that contains the action is started, in the **Enabled** box, select the option. To prevent the action from running when the policy or workflow that contains the action is started, clear this option.

   ⓘ Note: When you clear the **Enabled** option, actions that occurs after a disabled action do not start, even if the subsequent options are enabled.

5. From the **Action Type** list, select **Backup**.
6. From the secondary action list, select the backup type, for example, **Traditional**.
7. If you create the action as part of the workflow configuration, the workflow appears automatically in the **Workflow** box and the box is dimmed.
8. Specify the order of the action in relation to other actions in the workflow:
   - If the action is part of a sequence of actions in a workflow path, in the **Previous** box, select the action that should precede this action.
   - If the action should run concurrently with an action, in the **Previous** box, select the concurrent action, and then select the **Concurrent** checkbox.
9. Specify a weekly, monthly, or reference schedule for the action:
   - To specify a schedule for each day of the week, select **Define** option under **Select Schedule** and period as **Weekly by day**.
   - To specify a schedule for each day of the month, select **Define** option under **Select Schedule** and period as **Monthly by day**.
   - To specify a customized schedule to the action, select **Select** option under **Select Schedule** and choose a customized schedule using the drop down menu that is already created under NSR schedule resource.
10. To specify the backup level to perform when **Define** option under **Select Schedule** is selected, click the icon on each day. If it is Select option under **Select Schedule**, choose the customized NSR schedule using the drop down, after specifying the backup level within the NSR schedule resource.

    The following table provides details about the backup level that each icon represents.

Table 7 Schedule icons

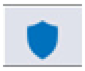
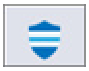
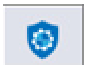
Icon	Label	Description
	**Full**	Perform a full backup on this day. Full backups include all files, regardless of whether the files changed.
	**Incr**	Perform an incremental backup on this day. Incremental backups include files that have changed since the last backup of any type (full or incremental).
	**Cumulative Incr**	Perform a cumulative incremental backup. Cumulative incremental backups include files that have changed since the last full backup.

Table 7 Schedule icons (continued)

Icon	Label	Description
🛡	**Logs Only**	Perform a backup of only database transaction logs.
🛡	**Incremental Synthetic Full**	Perform an incremental synthetic backup on this day. An incremental synthetic full backup includes all data that changed since the last full backup and subsequent incremental backups to create a synthetic full backup.
🛡	**Skip**	Do not perform a backup on this day.

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

11. Click **Next**.

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

12. From the **Destination storage node** box, select the storage node that contains the devices on which to store the backup data.

13. From the **Destination pool** box, select a pool that contains the devices on which to store the backup data.

14. From the **Retention** boxes, specify the amount of time to retain the backup data.

    After the retention period expires, the save set is removed from the client file index and marked as recyclable in the media database during an expiration server maintenance task.

15. From the **Client Override Behavior** box, specify how NetWorker uses certain client configuration attributes that perform the same function as attributes in the Action resource:

    - **Client Can Override**—The values in the Client resource for **Schedule**, **Pool**, **Retention policy**, and the **Storage Node** attributes take precedence over the values that are defined in the equivalent Action resource attributes.

      > ⓘ **Note:** If the NetWorker policy action schedule is set to the `Skip` backup level, the **Client can Override** option is not honored. For NetWorker to consider the **Client can Override** option, change the action schedule to a different level.

    - **Client Can Not Override**—The values in the Action resource for the **Schedule**, **Destination Pool**, **Destination Storage Node**, and the **Retention** attributes take precedence over the values that are defined in the equivalent Client resource attributes.

    - **Legacy Backup Rules**—This value only appears in actions that are created by the migration process. The updating process sets the **Client Override Behavior** for the migrated backup actions to **Legacy Backup Rules**.

16. Select the **Apply DD Retention Lock** checkbox to enable retention lock for the save sets included in this backup action. Note that the device used for backing up these save sets must also have DD Retention lock enabled in the **Device Properties** window or during device creation.

17. In the **DD Retention Lock Time** box, specify the duration the save sets will remain on the Data Domain device before the retention lock expires. During this time, these save sets

cannot be overwritten, modified, or deleted for the duration of the retention period, although the backups can be mounted and unmounted. The retention time period set here must fall within the minimum and maximum values set for the Data Domain Mtree, and should be lower than or equal to the NetWorker Retention Period.

18. Click **Next**.

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

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

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

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

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

21. In the **Inactivity Timeout** field, specify the maximum number of minutes that a job run by an action can try to respond to the server.

    If the job does not respond within the specified time, the server considers the job a failure and NetWorker retries the job immediately to ensures that no time is lost due to failures.

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

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

22. In the **Parallelism** field, specify the maximum number of concurrent operations for the action. This is applicable if multiple rollover is implemented at an action level.

23. From the **Failure Impact** list, specify what to do when a job fails:

    - To continue the workflow when there are job failures, select **Continue**.
    - To abort the current action if there is a failure with one of the jobs, but continue with subsequent actions in the workflow, select **Abort action**.

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

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

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

25. From the **Hard Limit** list, select the amount of time after the action starts to begin terminating activities. The default value of 0 (zero) indicates no amount of time.

26. Optional, in **Start Time** specify the time to start the action.

    Use the spin boxes to set the hour and minute values, and select one of the following options from the drop-down list:

    - **Disabled**—Do not enforce an action start time. The action will start at the time defined by the workflow.
    - **Absolute**—Start the action at the time specified by the values in the spin boxes.
    - **Relative**—Start the action after the period of time defined in the spin boxes has elapsed after the start of the workflow.

27. (Optional) Configure overrides for the task that is scheduled on a specific day.

    To specify the month, use the navigation buttons and the month list box. To specify the year, use the spin boxes. You can set an override in the following ways:

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

    > **Note:**
    >
    > - You can edit or add the rules in the **Override** field.
    > - To remove an override, delete the entry from the **Override** field.
    > - If a schedule is associated to an action, then override option is disabled.

28. From the **Send Notifications** list box, select whether to send notifications for the action:

    - To use the notification configuration that is defined in the Policy resource to send the notification, select **Set at policy level**.
    - To send a notification on completion of the action, select **On Completion**.
    - To send a notification only if the action fails to complete, select **On Failure**.

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

    The default notification action is to send the information to the `policy_notifications.log` file. By default, the `policy_notifications.log` file is located in the `/nsr/logs` directory on Linux and in the `C:\Program Files\EMC NetWorker\nsr\logs` folder on Windows.

    Use the default mailer program on Linux to send email messages or the `smtpmail` application on Windows:

    - To send notifications to a file, type the following command, where `policy_notifications.log` is the name of the file:

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

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

      ```
      mail -s subject recipient
      ```

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

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

  where:

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

30. Click **Next**.

    The **Action Configuration Summary** page appears.

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

After you finish

(Optional) Create a clone action to automatically clone the save sets after the backup. A clone action is the only supported action after a backup action in a workflow.

Creating a clone action

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

Before you begin

When cloning to or from a Cloud Tier device, the source and destination devices must reside on the same mtree.

Procedure

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

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

   The **Policy Action** wizard opens on the **Specify the Action Information** page.

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

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

   - Legal Characters: _ : - + = # , . % @
   - Illegal Characters: /*?[]()$!^;'"`~><&|{}

3. In the **Comment** field, type a description for the action.

4. To ensure that the action runs when the policy or workflow that contains the action is started, in the **Enabled** box, select the option. To prevent the action from running when the policy or workflow that contains the action is started, clear this option.

   > ⓘ **Note:** When you clear the **Enabled** option, actions that occurs after a disabled action do not start, even if the subsequent options are enabled.

5. From the **Action Type** list, select **Clone**.

6. If you create the action as part of the workflow configuration, the workflow appears automatically in the **Workflow** box and the box is dimmed.
7. Specify the order of the action in relation to other actions in the workflow:
   - If the action is part of a sequence of actions in a workflow path, in the **Previous** box, select the action that should precede this action.
   - If the action should run concurrently with an action, in the **Previous** box, select the concurrent action, and then select the **Concurrent** checkbox.
8. Specify a weekly, monthly, or reference schedule for the action:
   - To specify a schedule for each day of the week, select **Define** option under **Select Schedule** and period as **Weekly by day**.
   - To specify a schedule for each day of the month, select **Define** option under **Select Schedule** and period as **Monthly by day**.
   - To specify a customized schedule to the action, select **Select** option under **Select Schedule** and choose a customized schedule using the drop down menu that is already created under NSR schedule resource.
9. Specify the days to perform cloning:
   - To clone on a specific day, click the **Execute** icon on the day.
   - To skip a clone on a specific day, click the **Skip** icon on the day.
   - To check connectivity every day, select **Execute** from the list, and then click **Make All**.

   The following table provides details on the icons.

   Table 8 Schedule icons

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

10. Click **Next**.

    The **Specify the Clone Options** page appears.
11. In the **Data Movement** group box, define the volumes and devices for the source data and the clone data.

    a. From the **Source Storage Node** list, select the storage node host that contains the save set data in which to clone.

    b. From the **Destination Storage Node** list, select the storage node host on which to store the cloned save sets.

    ⓘ Note: To clone to a DD Cloud Tier device, the source and destination storage node devices must reside on the same mtree.

    c. In the **Delete source save sets after clone completes** box, select the option to instruct NetWorker to move the data from the source volume to the destination volume after clone operation completes. This is equivalent to staging the save sets.

    d. From the **Destination pool** list, select a clone pool.

    To clone to a DD Cloud Tier device, select a Cloud Tier pool.

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

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

12. Select the **Apply DD Retention Lock** checkbox to enable Retention Lock for the save sets included in this clone action. Note that the device used for cloning these save sets must also have DD Retention lock enabled in the **Device Properties** window or during device creation.

13. In the **DD Retention Lock Time** box, specify the duration the save sets will remain on the Data Domain device before the Retention Lock expires. During this time, these save sets cannot be overwritten, modified, or deleted for the duration of the retention period, although the device with the cloned backup can be mounted and unmounted. The retention time period set here must fall within the minimum and maximum values set for the Data Domain Mtree, and should be lower than or equal to the NetWorker Retention Period.

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

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

- **Do Not Filter**—NetWorker inspects the save sets in the media database to create a clone save set list that meets the time filter criteria.
- **Accept**—The clone save set list includes save sets that are saved within the time range and meet all the other defined filter criteria.
- **Reject**—The clone save set list does not include save sets that are saved within the time range and meet all the other defined filter criteria.

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

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

ⓘ **Note:** For NAS device, only Snapshot save set is applicable.

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

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

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

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

  ⓘ **Note:** For NAS device, only full backup level is applicable.

15. Click **Next**.

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

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

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

17. In the **Parallelism** field, specify the maximum number of concurrent operations for the action. This is applicable if multiple rollover is implemented at an action level.
18. From the **Failure Impact** list, specify what to do when a job fails:
    - To continue the workflow when there are job failures, select **Continue**.
    - To abort the current action if there is a failure with one of the jobs, but continue with subsequent actions in the workflow, select **Abort action**.

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

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

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

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

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

    The default notification action is to send the information to the `policy_notifications.log` file. By default, the `policy_notifications.log` file is located in the `/nsr/logs` directory on Linux and in the `C:\Program Files\EMC NetWorker\nsr\logs` folder on Windows.

    Use the default mailer program on Linux to send email messages or the `smtpmail` application on Windows:

- To send notifications to a file, type the following command, where `policy_notifications.log` is the name of the file:

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

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

  ```
  mail -s subject recipient
  ```

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

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

  where:

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

21. From the **Soft Limit** list, select the amount of time after the action starts to stop the initiation of new activities. The default value of 0 (zero) indicates no amount of time.
22. From the **Hard Limit** list, select the amount of time after the action starts to begin terminating activities. The default value of 0 (zero) indicates no amount of time.
23. Optional, in **Start Time** specify the time to start the action.

    Use the spin boxes to set the hour and minute values, and select one of the following options from the drop-down list:

    - **Disabled**—Do not enforce an action start time. The action will start at the time defined by the workflow.
    - **Absolute**—Start the action at the time specified by the values in the spin boxes.
    - **Relative**—Start the action after the period of time defined in the spin boxes has elapsed after the start of the workflow.

24. (Optional) Configure overrides for the task that is scheduled on a specific day.

    To specify the month, use the navigation buttons and the month list box. To specify the year, use the spin boxes. You can set an override in the following ways:

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

      > **Note:**
      >
      > - You can edit or add the rules in the **Override** field.
      > - To remove an override, delete the entry from the **Override** field.
      > - If a schedule is associated to an action, then override option is disabled.

25. Click **Next**.

    The **Action Configuration Summary** page appears.

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

After you finish

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

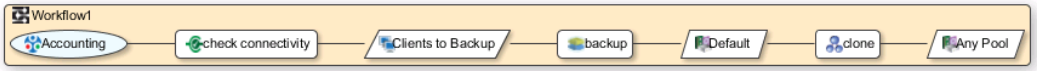
> **Note:** To clone data from a Cloud Tier device, the destination storage node must contain DDBoost devices that reside on the same mtree as the Cloud Tier device.

Visual representation of workflows

After you create actions for a workflow, in the Administration interface, you can see a map provides a visual representation of the actions on the right side of the **Protection** window.

The following figure illustrates the visual representation of a sample workflow for a traditional backup.

Figure 45 Visual representation of a workflow



The oval icon specifies the group to which the workflow applies. The rounded rectangle icons identify actions. The parallelogram icons identify the destination pool for the action.

- You can adjust the display of the visual representation by right-clicking and selecting one of the following options:
  - **Zoom In**—Increase the size of the visual representation.
  - **Zoom Out**—Decrease the size of the visual representation.
  - **Zoom Area**—Limit the display to a single section of the visual representation.
  - **Fit Content**—Fit the visual representation to the window area.
  - **Reset**—Reset the visual representation to the default settings.
  - **Overview**—View a separate dialog box with a high-level view of the visual representation and a legend of the icons.
- You can view and edit the properties for the group, action, or destination pool by right-clicking the icon for the item, and then select **Properties**.
- You can create a group, action, or destination pool by right-clicking the icon for the item, and then select **New**.

Cloning with Data Domain (DD Boost)

As with other NetWorker devices, you can use Data Domain device types to perform clone operations. You can clone single save sets or the entire Data Domain volume from a Data Domain device. You can also use the Data Domain device as the target device, to receive cloned data.

Cloning works differently for deduplication devices. You can perform clone-controlled replication (CCR), or optimized cloning of data, from one Data Domain system to another. Or you can clone data from a Data Domain device to tape or to any other device type.

ⓘ Note: To use Data Domain with NetWorker, the NetWorker server hostname should be in lower case. Data Domain functions with lowercase and DD Cloud tier operations fails if it is mixed case.

Clone formats

Yo can clone data that is stored on a Data Domain device in one of two formats, which depend on the target media device:

- CCR format
- Regular clone format

Clone-controlled replication format

When you clone data to a target Data Domain device, typically at a remote location, the data retains the deduplication format. This format is known as clone-controlled replication (CCR), or as an optimized clone.

CCR uses the native Data Domain replication feature to copy data from one Data Domain system to another.

CCR uses a special Data Domain API and differs from standard directory level replication, which is also supported. The clone is created quickly and uses low bandwidth and low storage capacity.

You can use a clone that is created in this format 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 supports immediate cloning with CCR. Immediate cloning means that you can clone each save set when the backup completes instead of waiting until the backup completes for all save sets in the action. Cloning operations can complete sooner because they can now run in parallel instead of sequentially. Performance gains are most noticeable when there are many backup save sets in the backup queue or when there are many save sets of different sizes.

You can set up immediate cloning by specifying the clone action as concurrent to the previous backup action in a policy workflow.

Regular clone format

When you clone the data on the Data Domain device to a traditional disk or tape, the clone process reverts the data to the native non-deduplicated format, known as "regular clone" format.

NetWorker requires the data on traditional disk or tape to be in regular clone format to ensure that the data is completely recoverable, 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.

CCR requirements

Before you use CCR to clone data, ensure that following requirements are met.

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 all of the host identifiers in the **Aliases** attribute.

  - Fully-qualified domain name
  - Short name
  - Aliases
  - IP address

    Note: If you use an `nsrclone` command to perform an optimized clone from a host that is not the NetWorker server, then you must specify the primary hostname of the NetWorker server by using the -S option. The primary hostname of the NetWorker server is the name that appears 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.
5. Ensure that the source Data Domain device is mounted and available on the source storage node.
   If the source device is not mounted, then NetWorker will perform a regular, non-deduplicated clone. 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.
6. Ensure that the target Data Domain device is labeled for a clone pool, 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.
7. 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 the clone action, in the Destination pool attribute of the Action resource, select **newclonepool**.
   - For clones of entire volumes, Cloning by pools provides details.

Cloning by pools

To copy save sets from Data Domain storage to a Data Domain device, you must specify a pool. 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.

DD Boost clone and replication support

For additional data protection, you can use the NetWorker clone feature to copy save sets on a DD Boost device to a different location. A clone is a complete and independent copy of the data that you can use for data recovery or to create additional clones. You can clone single save sets or the entire volume of a DD Boost device. A clone retains the original NetWorker browse and retention policies by default.

You can configure clones to run immediately after each save set completes, or you can configure clones to run in an independently defined maintenance window after the entire policy completes in the main backup window.

Clone formats

The type of NetWorker clone you produce depends on the type of storage media you use for the clone. NetWorker will use either CCR when cloning to DD Boost devices or a normal clone when cloning to conventional storage media.

CCR format

When NetWorker clones data from a source DD Boost device to a target DD Boost device, usually at a geographically distant location, the operation uses CCR, also known as optimized clone or DD format clone. CCR is a fast process that uses low bandwidth, multiple parallel sessions, and low storage capacity. You can use CCR clones for data recovery or to create additional copies with minimal impact on the primary operations of production, backup, or recovery.

CCR operations use only IP connectivity between DD Boost devices on separate Data Domain systems, whether you have configured the participating devices for FC or IP.

For CCR operations on the same Data Domain system, Dell EMC recommends that you replicate the data between two different SUs (MTrees), so you can apply different retention policies and manage the data independently. When you perform CCR operations to disks that reside within the same Data Domain system, CCR uses fast copy operation.

During the CCR process, the storage node reviews the incoming clone for data that NetWorker has already stored on the target DD Boost device. The storage node stores only unique data that does not exist on the device.

Normal clone format

When NetWorker clones data from a DD Boost device to conventional media, for example, or tape, the data reverts to the non-deduplicated format. This procedure creates a normal clone. The normal clone format is necessary for the data on conventional disk or tape storage to be fully recoverable, for example, for disaster recovery, without the need of a Data Domain system.

Native Data Domain replication considerations

Dell EMC recommends that you do not use native Data Domain replication operations to clone data. Native replication is normally used to copy deduplicated data stored in CIFS, NFS, or VTL formats from one Data Domain system to another for disaster recovery purposes. Native replication clones data independently of NetWorker and DD Boost, and the NetWorker software cannot track or control native replication operations.

An exception would be to seed a new Data Domain system by collection replication to assist the migration of existing data. Migration versus native Data Domain replication on page 184 provides details.

ⓘ **Note:** If you use Data Domain replication for non-DD Boost directories on the same system, ensure that the system and the network has enough capacity to enable NetWorker CCR operation with DD Boost devices.

Before you use native Data Domain replication with DD Boost devices review the following information:

- Directory replication (MTree replication) does not support DD Boost devices.
- Collection replication, which is the replication of the entire stored contents of a Data Domain system, renders DD Boost devices as read-only. This operation will replicate all DD Boost devices and the stored data onto a target Data Domain system. You cannot use the replicated DD Boost data for other replication operations, such as NetWorker CCR.

Note: When you perform a collection replication of a Data Domain system, the NetWorker software is not aware of any DD Boost devices on that system. Additional procedures, tests, and qualifications are required to configure NetWorker to detect the devices and enable data recovery of the replicated DD Boost data. Contact Dell EMC Professional services for assistance.

Data Domain Automated Multi-streaming (AMS)

The AMS feature improves cloning performance for large savesets when you use high bandwidth networks. Previously when you replicated savesets between two Data Domain devices on different machines, the replication process used to take longer in NetWorker. AMS significantly speeds up replication between DDRs by splitting up large files (files whose sizes are roughly greater than 3.5 GB) into multiple smaller 2 GB slices, replicating the slices individually, and finally re-creating the original large file on the destination DDR using those slices.

NetWorker 8.2.3 and NetWorker 9.0.1 and later features enhancements for clone-controlled replication (CCR), also known as DD to DD Managed File Replication. Also, enhancements to load balancing so that the load (save sets to clone) is spread evenly across the multi-threaded `nsrclone` process were implemented.

By default the AMS feature is disabled. You can turn on the feature by changing the command to ams_enabled=**`yes`** An example of how you can enable AMS is below:

```
racdd098:/nsr/debug # cat nsrcloneconfig
max_total_dd_streams=256
ams_enabled=yes
ams_slice_size_factor=31
ams_preferred_slice_count=0
ams_min_concurrent_slice_count=1
ams_max_concurrent_slice_count=20
max_threads_per_client=256
ams_force_multithreaded=yes
```

Note: Both Data Domains should be connected through a 10GB network.

Configuring the Data Domain CCR environment

This section describes how to configure the network environment for CCR

Before you begin

- To use Data Domain encryption, global compression, or low-bandwidth optimization, enable these configurations on both the source and target Data Domain systems.

  Note: If any of these configurations do not match on both the source and target Data Domain systems, clone operations will fail.

  The *Data Domain Operating System Administration Guide* provides details on these settings.
- On the NetWorker server and both storage nodes, configure the Client resource **Aliases** field on the **Globals 1 of 2** tab with a list of all the names and aliases in use for the CCR. Include the fully qualified name, short name, aliases, and IP address.
- Select or create a target pool for the CCR, configured for **Backup Clone** type with the **Media Type Required** field set to **Data Domain**.
  If a DD Boost device that is targeted by the pool is not available during a CCR, and the media type required specifies Data Domain, then NMC displays a `Media Waiting` message.

ⓘ **Note:** Do not use the Default Clone Pool. You cannot change the **Media type required** setting.

About this task

Complete the following steps to configure the network environment for CCR:

Procedure

1. Ensure that you have enabled valid licenses to the Data Domain systems that you will use for CCR operations, including a Replication license.
2. Ensure that the source and destination storage nodes are within the same datazone. A single NetWorker server must manage the clone operations and maintain the retention policies for all cloned copies. The server also monitors and reports on the storage operations.
3. Ensure Ethernet IP connectivity between the source and destination Data Domain systems. CCR occurs only over TCP/IP connectivity. If a DD Boost device participating in the CCR also has an FC connection, ensure IP access to the DD Boost device.
4. Ensure that you map the Data Domain FC server name to the IP address, if the Domain FC and IP hostnames differ.

   ⓘ **Note:** Do not use connections with ifgroup links for clone operations.

   Data Domain FC and IP hostnames are the same by default but they can be different. If they are different you must map the host Data Domain FC server name to its own IP address as follows:

   a. Open the Data Domain Enterprise Manager, and navigate to the **Data Management** > **DD Boost**. The Data Domain **Server Name** appears on the **Fibre Channel** tab.

      Alternatively, type the following command:

      ```
      ddboost fc dfc-server-name show
      ```

   b. Associate this server name to the IP address in the `/etc/hosts` file with the following command:

      ```
      net hosts add fc_server_name IP_address
      ```

      For example, if the Data Domain system has the IP address 10.99.99.99 and the IP hostname dd555-5.lss.mcm.com, and the DFC server name is dd-tenendo, then type the following command:

      ```
      net hosts add dd-tenendo 10.99.99.99
      ```

5. Mount the source DD Boost device on the source storage node.
6. Mount the target DD Boost device on the target storage node. The pool for the device must specify **Backup Clone** pool type.
7. Ensure that the target clone pool is properly specified for the clone method you use. Clone save sets will be written to this pool. You may need to use multiple or mixed approaches for control and flexibility.

   The following example use myccrpool as the name of a clone pool you created:

   - For CLI clone operations, type the command `nsrclone -b myccrpool`.

Strategies for cloning

You can use scheduled cloning or action based (automatic) cloning to manage your data.

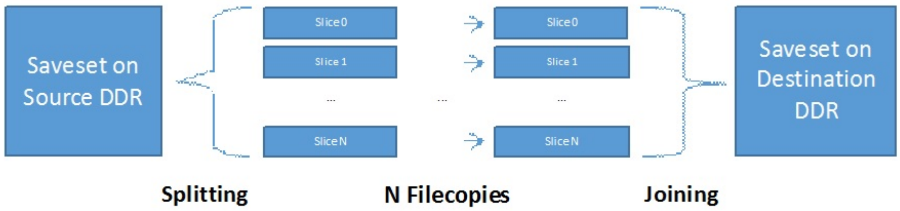
- Scheduled cloning—You can have a policy, and a workflow followed by a clone action. The workflow is associated with a dynamic group. In other words, a Query or Save set protection group.
- Action based (automatic) cloning—You can have a policy, and a workflow followed by a backup and a clone action. The clone action can be configured as concurrent or sequential.
    - Sequential—When the backup action configured for a policy or workflow is triggered, backup copies are created in the selected backup pool. However, the clone action is triggered only after backup copies are created for all the selected save sets. For example, If there are save sets numbered 1 to 100, backup copies are created in order. The clone action is triggered only after the backup copy is created for save set 100.
      ⓘ **Note:** Sequential cloning is the preferred cloning method.
    - Concurrent—When the backup action configured for a policy or workflow is triggered, backup copies are created in the selected backup pool. The clone action is triggered even if only a single back up copy is created from the selected save sets. For example, If there are save sets numbered 1 to 100, backup copies are created in order. The clone action for save set 1 is triggered as soon as the backup copy for save set 1 is created. However, for performance optimization, clones for save sets are triggered in batches.

You can also use automated multi-streaming (AMS) when cloning your data to speed up the replication process.

If you are replicating save sets between two Data Domain devices on different machines, replication using NetWorker takes longer because each save set uses a single stream. The use of automated multi-streaming (AMS) splits up large files (files larger than 3.5 GiB) into multiple smaller 2 GiB slices, replicates those slices individually, and recreates the original large file on the destination DDR using those slices.

The following diagram illustrates replication using AMS.

Figure 46 Replication using AMS



AMS is supported only if:

- Both the source and destination Data Domain systems support the virtual synthetic capability (DDOS 5.5 and later). This can be validated through `ddboost option show` command as shown below:

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

```
global-authentication-mode     none
global-encryption-strength     none
```

- The save set file being copied is large enough for the use of AMS to provide an improvement over normal replication.
- All save set types other than VBA, vProxy, Hyper-V, BBB, and synthetic full. The exception is for Microsoft NMM Exchange module save sets, where AMS is used even though it uses BBB and synthetic full.

Enable AMS, if the underlying bandwidth between two DDRs is 10Gbps. Because the use of AMS creates multiple streams, there must be enough bandwidth between the two DDRs being used for the clone workflow.

The `nsrcloneconfig` file enables you to add debug flags, control cloning sessions, and use the AMS functionality. It must be manually created under the `/nsr/debug` folder.

By default, AMS is disabled. To enable AMS, ensure that the `ams_enabled` flag is set to Yes.

The following table describes the `nsrcloneconfig` file details and their default values.

Table 9 `nsrcloneconfig` file details

Settings	Default value	Description
ams_enabled	Yes	Enables or disables AMS support. The value can be Yes or No.
ams_slice_size_factor	31	Allows you to change the slice size factor value. The slice size factor corresponds to the size of the slices desired, specified by a number of bits. For example, if the slice size factor is 28, the desired slice size is 2^28, or 256 MiB. The default value is 31, meaning the desired slice size is 2^31, or 2 GiB. The default value of 31 provides the best performance during chopping and joining.
ams_preferred_slice_count	0	Allows you to change the preferred slice count. There is no maximum value.
ams_min_concurrent_slice_count	1	Allows you to increase the minimum number of concurrent file copies. If the specified value is less than the default minimum value, the default value is used.
ams_max_concurrent_slice_count	20	Allows you to decrease the maximum number of concurrent file copies. If the specified value exceeds the default maximum value, the default value is used.
ams_force_multithreaded	No	Force AMS to use threads even when the DDRs support multi-file copies. Because the multi-file workflow is faster, this is only useful for explicitly testing the multithreaded workflow. The value can be Yes or No.
Debug	9	

ⓘ **Note:** The Backup Data Management chapter describes how you can clone save sets manually by using the `nsrclone` command.

Road map for configuring a new cloning data protection policy

This road map provides a high level overview of how to configure a new policy for clone operations.

Before you begin

Configure the backup policy to back up the data that is cloned.

Procedure

1. Create a group to define the data to clone.
2. Create a policy. When you create a policy, you specify the name and notification settings for the policy.
3. Within the policy, create a workflow. When you create a workflow, you specify the name of the workflow, the schedule for running the workflow, notification settings for the workflow, and the protection group to which the workflow applies.
4. Create one or more clone actions for the workflow.

Protection groups for a cloning workflow

You can use two types of protection groups to clone save sets in a workflow that are separate from backup workflows. The type of protection group that you use depends on the way that you plan to configure the workflow.

Use a save set group or a query group to specify a list of save sets if cloning occurs as the head action in a cloning workflow:

- Save set group—Use a save set group in clone-only workflows where you want to clone a specific list of save sets. Save set groups are similar to the manual clone operations in NetWorker 8.2.x and earlier.
- Query group—Use a query group in clone-only workflows where you want to clone save sets on an ongoing basis, based on the save set criteria that you define. Query groups are similar to the scheduled clone operations in NetWorker 8.2.x and earlier.

ⓘ **Note:** To clone save sets in a backup workflow, use basic client group or a dynamic client group. Strategies for traditional backups provides detailed information about how to create clone actions in a traditional backup workflow.

Create multiple protection groups to perform cloning in different ways as part of separate workflows, or to perform cloning for different save sets on different schedules. For example:

- Create a basic client group for a workflow that performs a traditional backup of the a client file system followed by cloning of the save sets that result from the backup. In this case, concurrent cloning can be enabled.
- Create a query group that identifies full save sets in the last two days to clone.

Creating a save set group

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

Before you begin

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

Procedure

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

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

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

   - Legal Characters: _ : - + = # , . % @
   - Illegal Characters: /*?[]()$!^;'"`~><&|{}

   > **Note:** After you create a group, the **Name** attribute is read-only.
4. From the **Group Type** list, select **Save Set ID List**.
5. In the **Comment** field, type a description of the group.
6. (Optional) To associate the group with a workflow, from the **Workflow (Policy)** list, select the workflow.

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

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

Creating a query group

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

Procedure

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

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

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

   - Legal Characters: _ : - + = # , . % @
   - Illegal Characters: /*?[]()$!^;'"`~><&|{}

   > **Note:** After you create a group, the **Name** attribute is read-only.
4. From the **Group Type** list, select **Save Set Query**.
5. In the **Comment** field, type a description of the group.
6. (Optional) To associate the group with a workflow, from the **Workflow (Policy)** list, select the workflow.

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

7. Specify one or more of the save set criteria in the following table.

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

   Table 10 Save set criteria

Criteria	Description
Date and time range	Specify the start date and time range for the save sets. To specify the current date and time as the end date for the range, select **Up to now**. To specify a time period, select **Up to**.
Backup level	In the **Filter save sets by level** section, next to the backup level for the save set, select the **full** checkbox. ⓘ Note: Only the **full** backup level is applicable for network-attached storage (NAS) devices.
Limit the number of clones	Specify the number for the limit in the **Limit number of clones** list. The clone limit is the maximum number of clone instances that can be created for the save set. By default, the value is set to 1, and cannot be changed for NAS or Block. ⓘ Note: When this criteria is set to 1, which is the default value, you may experience volume outage issues with Data Domain and advanced file type devices.
Client	Next to one or more client resources that are associated with the save set in the **Client** list, select the checkbox.
Policy	Next to the policy used to generate the save set in the **Policy** list, select the checkbox.
Workflow	Next to the workflow used to generate the save set in the **Workflow** list, select the checkbox.
Action	Next to the action used to generate the save set in the **Action** list, select the checkbox.
Group	Next to the group associated with the save set in the **Group** list, select the checkbox.
Pools	Next to the media pool on which the save set is stored in the **Pools** list, select the checkbox. ⓘ Note: You cannot select Pools for NAS.
Name	In the **Filter save sets by name** field, specify the name of the save set. ⓘ Note: You cannot use wildcards to specify the save set name.

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

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

Creating a policy

Procedure

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

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

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

   - Legal Characters: _ : - + = # , . % @
   - Illegal Characters: /*?[]()$!^;'"`~><&|{}

   Note: After you create a policy, the **Name** attribute is read-only.
4. In the **Comment** field, type a description for the policy.
5. From the **Send Notifications** list, select whether to send notifications for the policy:
   - To avoid sending notifications, select **Never**.
   - To send notifications with information about each successful and failed workflow and action, after the policy completes all the actions, select **On Completion**.
   - To send a notification with information about each failed workflow and action, after the policy completes all the actions, select **On Failure**.
6. In the **Send notification** attribute, when you select the **On Completion** option or **On failure** option, the **Command** box appears. Use this box to configure how NetWorker sends the notifications. You can use the `nsrlog` command to send the notifications to a log file or you can send an email notification.

   The default notification action is to send the information to the `policy_notifications.log` file. By default, the `policy_notifications.log` file is located in the `/nsr/logs` directory on Linux and in the `C:\Program Files\EMC NetWorker\nsr\logs` folder on Windows.

   To send email messages or the `smtpmail` application on Windows, use the default mailer program on Linux:

   - To send notifications to a file, type the following command, where `policy_notifications.log` is the name of the file:

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

     ```
     mail -s subject recipient
     ```
   - For NetWorker Virtual Edition (NVE), to send an email notification, type the following command:

     ```
     /usr/sbin/sendmail -v recipient_email "subject_text"
     ```
   - On Windows, to send a notification email, type the following command:

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

     where:

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

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

After you finish

Create the workflows and actions for the policy.

Create a workflow for a new policy in NetWorker Administration

Procedure

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

   The maximum number of allowed characters for the **Name** field is 64.

   - Legal Characters: _ : - + = # , . % @
   - Illegal Characters: /*?[]()$!^;'"`~><&|{}

5. In the **Comment** box, type a description for the workflow.

   The maximum number of allowed characters for the **Comment** field is 128.

6. From the **Send Notifications** list, select how to send notifications for the workflow:

   - To use the notification configuration that is defined in the policy resource to specify when to send a notification, select **Set at policy level**.
   - To send notifications with information about each successful and failed workflow and action, after the workflow completes all the actions, select **On Completion**.
   - To send notifications with information about each failed workflow and action, after the workflow completes all the actions, select **On Failure**.

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

   The default notification action is to send the information to the `policy_notifications.log` file. By default, the `policy_notifications.log` file is located in the `/nsr/logs` directory on Linux and in the `C:\Program Files\EMC NetWorker\nsr\logs` folder on Windows.

   Use the default mailer program on Linux to send email messages, or use the `smtpmail` application on Windows:

   - To send notifications to a file, type the following command, where `policy_notifications.log` is the name of the file:

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

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

  ```
  mail -s subject recipient
  ```

- For NetWorker Virtual Edition (NVE), to send an email notification, type the following command:

  ```
  /usr/sbin/sendmail -v recipient_email "subject_text"
  ```

- On Windows, type the following command:

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

  where:

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

8. In the **Running** section, perform the following steps to specify when and how often the workflow runs:

   a. To ensure that the actions that are contained in the workflow run when the policy or workflow starts, in the **Enabled** box, leave the option selected. To prevent the actions in the workflow from running when the policy or workflow that contains the action starts, clear this option.

   b. To start the workflow at the time that is specified in the **Start time** attribute, on the days that are defined in the action resource, in the **AutoStart Enabled** box, leave the option selected. To prevent the workflow from starting at the time that is specified in the **Start time** attribute, clear this option.

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

      The default value is 9:00 PM.

   d. To specify how frequently to run the actions that are defined in the workflow over a 24-hour period, use the **Interval** attribute spin boxes. If you are performing transaction log backup as part of application-consistent protection, you must specify a value for this attribute in order for incremental transaction log backup of SQL databases to occur.

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

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

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

      For example, if the **Start Time** is 7:00 PM, the **Interval** is 1 hour, and the **Interval End** is 11:00 PM., then the workflow automatically starts every hour beginning at 7:00 PM. and the last start time is 11:00 PM.

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

After you finish

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

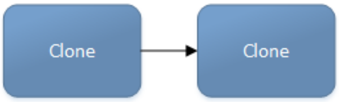
Workflows for scheduled cloning

A workflow can contain one or more clone actions.

Supported workflow path from a clone action

Another clone action is the only supported action after a clone action.

Figure 47 Workflow path from a clone action



Creating a clone action

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

Before you begin

When cloning to or from a Cloud Tier device, the source and destination devices must reside on the same mtree.

Procedure

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

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

   The **Policy Action** wizard opens on the **Specify the Action Information** page.

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

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

   - Legal Characters: _ : - + = # , . % @
   - Illegal Characters: /*?[]()$!^;'"`~><&|{}

3. In the **Comment** field, type a description for the action.

4. To ensure that the action runs when the policy or workflow that contains the action is started, in the **Enabled** box, select the option. To prevent the action from running when the policy or workflow that contains the action is started, clear this option.

   > ⓘ **Note:** When you clear the **Enabled** option, actions that occurs after a disabled action do not start, even if the subsequent options are enabled.

5. From the **Action Type** list, select **Clone**.

6. If you create the action as part of the workflow configuration, the workflow appears automatically in the **Workflow** box and the box is dimmed.

7. Specify the order of the action in relation to other actions in the workflow:

- If the action is part of a sequence of actions in a workflow path, in the **Previous** box, select the action that should precede this action.
- If the action should run concurrently with an action, in the **Previous** box, select the concurrent action, and then select the **Concurrent** checkbox.

8. Specify a weekly, monthly, or reference schedule for the action:

   - To specify a schedule for each day of the week, select **Define** option under **Select Schedule** and period as **Weekly by day**.
   - To specify a schedule for each day of the month, select **Define** option under **Select Schedule** and period as **Monthly by day**.
   - To specify a customized schedule to the action, select **Select** option under **Select Schedule** and choose a customized schedule using the drop down menu that is already created under NSR schedule resource.

9. Specify the days to perform cloning:

   - To clone on a specific day, click the **Execute** icon on the day.
   - To skip a clone on a specific day, click the **Skip** icon on the day.
   - To check connectivity every day, select **Execute** from the list, and then click **Make All**.

   The following table provides details on the icons.

   Table 11 Schedule icons

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

10. Click **Next**.

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

11. In the **Data Movement** group box, define the volumes and devices for the source data and the clone data.

    a. From the **Source Storage Node** list, select the storage node host that contains the save set data in which to clone.

    b. From the **Destination Storage Node** list, select the storage node host on which to store the cloned save sets.

    > ⓘ **Note:** To clone to a DD Cloud Tier device, the source and destination storage node devices must reside on the same mtree.

    c. In the **Delete source save sets after clone completes** box, select the option to instruct NetWorker to move the data from the source volume to the destination volume after clone operation completes. This is equivalent to staging the save sets.

    d. From the **Destination pool** list, select a clone pool.

    To clone to a DD Cloud Tier device, select a Cloud Tier pool.

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

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

12. Select the **Apply DD Retention Lock** checkbox to enable Retention Lock for the save sets included in this clone action. Note that the device used for cloning these save sets must also have DD Retention lock enabled in the **Device Properties** window or during device creation.

13. In the **DD Retention Lock Time** box, specify the duration the save sets will remain on the Data Domain device before the Retention Lock expires. During this time, these save sets cannot be overwritten, modified, or deleted for the duration of the retention period, although the device with the cloned backup can be mounted and unmounted. The retention time period set here must fall within the minimum and maximum values set for the Data Domain Mtree, and should be lower than or equal to the NetWorker Retention Period.

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

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

    - **Do Not Filter**—NetWorker inspects the save sets in the media database to create a clone save set list that meets the time filter criteria.
    - **Accept**—The clone save set list includes save sets that are saved within the time range and meet all the other defined filter criteria.
    - **Reject**—The clone save set list does not include save sets that are saved within the time range and meet all the other defined filter criteria.

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

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

    Note: For NAS device, only Snapshot save set is applicable.

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

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

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

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

ⓘ Note: For NAS device, only full backup level is applicable.

15. Click **Next**.

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

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

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

17. In the **Parallelism** field, specify the maximum number of concurrent operations for the action. This is applicable if multiple rollover is implemented at an action level.
18. From the **Failure Impact** list, specify what to do when a job fails:
    - To continue the workflow when there are job failures, select **Continue**.
    - To abort the current action if there is a failure with one of the jobs, but continue with subsequent actions in the workflow, select **Abort action**.

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

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

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

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

    The default notification action is to send the information to the `policy_notifications.log` file. By default, the `policy_notifications.log` file is located in the `/nsr/logs` directory on Linux and in the `C:\Program Files\EMC NetWorker\nsr\logs` folder on Windows.

    Use the default mailer program on Linux to send email messages or the `smtpmail` application on Windows:

    - To send notifications to a file, type the following command, where `policy_notifications.log` is the name of the file:

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

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

  ```
  mail -s subject recipient
  ```

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

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

  where:

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

21. From the **Soft Limit** list, select the amount of time after the action starts to stop the initiation of new activities. The default value of 0 (zero) indicates no amount of time.
22. From the **Hard Limit** list, select the amount of time after the action starts to begin terminating activities. The default value of 0 (zero) indicates no amount of time.
23. Optional, in **Start Time** specify the time to start the action.

    Use the spin boxes to set the hour and minute values, and select one of the following options from the drop-down list:

    - **Disabled**—Do not enforce an action start time. The action will start at the time defined by the workflow.
    - **Absolute**—Start the action at the time specified by the values in the spin boxes.
    - **Relative**—Start the action after the period of time defined in the spin boxes has elapsed after the start of the workflow.

24. (Optional) Configure overrides for the task that is scheduled on a specific day.

    To specify the month, use the navigation buttons and the month list box. To specify the year, use the spin boxes. You can set an override in the following ways:

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

      > **Note:**
      >
      > - You can edit or add the rules in the **Override** field.
      > - To remove an override, delete the entry from the **Override** field.
      > - If a schedule is associated to an action, then override option is disabled.

25. Click **Next**.

    The **Action Configuration Summary** page appears.

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

After you finish

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

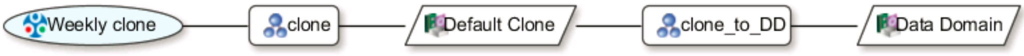
Note: To clone data from a Cloud Tier device, the destination storage node must contain DDBoost devices that reside on the same mtree as the Cloud Tier device.

Visual representation of a clone workflow

After you create actions for a workflow, in the Administration interface, you can see a map provides a visual representation of the actions on the right side of the **Protection** window.

The following figure illustrates the visual representation of a clone workflow.

Figure 48 Visual representation of a clone workflow



The oval icon specifies the group to which the workflow applies. The rounded rectangle icons identify actions. The parallelogram icons identify the destination pool for the action.

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

- You can adjust the display of the visual representation by right-clicking and selecting one of the following options:
  - **Zoom In**—Increase the size of the visual representation.
  - **Zoom Out**—Decrease the size of the visual representation.
  - **Zoom Area**—Limit the display to a single section of the visual representation.
  - **Fit Content**—Fit the visual representation to the window area.
  - **Reset**—Reset the visual representation to the default settings.
  - **Overview**—View a separate dialog box with a high-level view of the visual representation and a legend of the icons.
- You can view and edit the properties for the group, action, or destination pool by right-clicking the icon for the item, and then select **Properties**.
- You can create a group, action, or destination pool by right-clicking the icon for the item, and then select **New**.

Road map to add a clone workflow to an existing policy

This road map provides a high level overview of how to create a clone workflow and add the workflow to an existing backup policy.

Before you begin

Configure the backup policy to back up the data that is cloned.

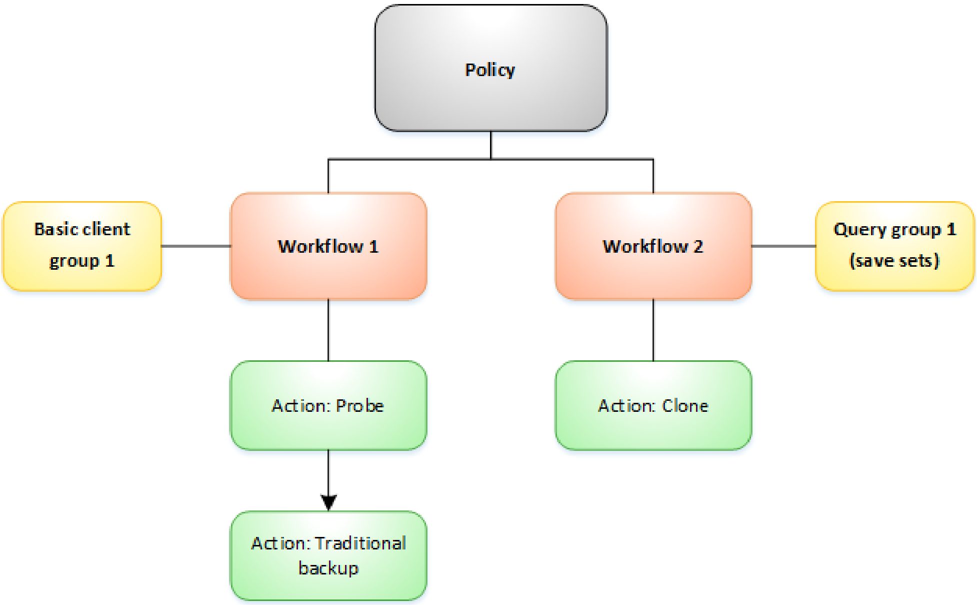
Procedure

1. Create a query or save set group to define the data to clone.
2. Add the new group to an existing policy.
3. Create a workflow in the existing policy.
4. Create one or more clone actions for the workflow.

Example: Creating a policy that has a separate workflow for cloning

The following figure provides a high level overview of the configuration of a policy that contains two workflows, one for backups and one to clone a list of save sets.

Figure 49 Example of a policy with separate workflows for backup and cloning



ⓘ **Note:** The amount of data and length of time that is required to complete the backup can impact the ability to clone data when the backup and clone workflows are in the same policy. For example, if the clone action starts before the backup action completes, there might not be any data yet to clone, or in other cases, only the save sets that completed at the start time of the workflow is taken into account. In both cases, NetWorker marks the Clone Workflow as successful, but there is no guarantee that all the data from the backup workflow was cloned.

Protection groups for a cloning workflow

You can use two types of protection groups to clone save sets in a workflow that are separate from backup workflows. The type of protection group that you use depends on the way that you plan to configure the workflow.

Use a save set group or a query group to specify a list of save sets if cloning occurs as the head action in a cloning workflow:

- Save set group—Use a save set group in clone-only workflows where you want to clone a specific list of save sets. Save set groups are similar to the manual clone operations in NetWorker 8.2.x and earlier.
- Query group—Use a query group in clone-only workflows where you want to clone save sets on an ongoing basis, based on the save set criteria that you define. Query groups are similar to the scheduled clone operations in NetWorker 8.2.x and earlier.

ⓘ **Note:** To clone save sets in a backup workflow, use basic client group or a dynamic client group. Strategies for traditional backups provides detailed information about how to create clone actions in a traditional backup workflow.

Create multiple protection groups to perform cloning in different ways as part of separate workflows, or to perform cloning for different save sets on different schedules. For example:

- Create a basic client group for a workflow that performs a traditional backup of the a client file system followed by cloning of the save sets that result from the backup. In this case, concurrent cloning can be enabled.
- Create a query group that identifies full save sets in the last two days to clone.

Creating a save set group

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

Before you begin

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

Procedure

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

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

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

   - Legal Characters: _ : - + = # , . % @
   - Illegal Characters: /*?[]()$!^;'"`~><&|{}

   Note: After you create a group, the **Name** attribute is read-only.
4. From the **Group Type** list, select **Save Set ID List**.
5. In the **Comment** field, type a description of the group.
6. (Optional) To associate the group with a workflow, from the **Workflow (Policy)** list, select the workflow.

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

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

Creating a query group

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

Procedure

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

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

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

   - Legal Characters: _ : - + = # , . % @

- Illegal Characters: /*?[]()$!^;'"`~><&|{}

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

4. From the **Group Type** list, select **Save Set Query**.
5. In the **Comment** field, type a description of the group.
6. (Optional) To associate the group with a workflow, from the **Workflow (Policy)** list, select the workflow.

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

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

Table 12 Save set criteria

Criteria	Description
Date and time range	Specify the start date and time range for the save sets. To specify the current date and time as the end date for the range, select **Up to now**. To specify a time period, select **Up to**.
Backup level	In the **Filter save sets by level** section, next to the backup level for the save set, select the **full** checkbox. **Note:** Only the **full** backup level is applicable for network-attached storage (NAS) devices.
Limit the number of clones	Specify the number for the limit in the **Limit number of clones** list. The clone limit is the maximum number of clone instances that can be created for the save set. By default, the value is set to 1, and cannot be changed for NAS or Block. **Note:** When this criteria is set to 1, which is the default value, you may experience volume outage issues with Data Domain and advanced file type devices.
Client	Next to one or more client resources that are associated with the save set in the **Client** list, select the checkbox.
Policy	Next to the policy used to generate the save set in the **Policy** list, select the checkbox.
Workflow	Next to the workflow used to generate the save set in the **Workflow** list, select the checkbox.
Action	Next to the action used to generate the save set in the **Action** list, select the checkbox.
Group	Next to the group associated with the save set in the **Group** list, select the checkbox.
Pools	Next to the media pool on which the save set is stored in the **Pools** list, select the checkbox. **Note:** You cannot select Pools for NAS.

Table 12 Save set criteria (continued)

Criteria	Description
Name	In the **Filter save sets by name** field, specify the name of the save set. ⓘ **Note:** You cannot use wildcards to specify the save set name.

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

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

Editing an existing policy to create a workflow and clone action

Use the **Policies** window to create a workflow and create the clone action.

Procedure

1. In the **Administration** window, click **Protection**.
2. In the expanded left pane, expand **Policies**, and then select the existing policy.
3. In the right pane, right-click in the workflow section and select **New**, and select **Properties**.

   The **New Workflow** dialog box appears.
4. In the **Name** field, type the name of the workflow.

   The maximum number of allowed characters for the **Name** field is 64.

   - Legal Characters: _ : - + = # , . % @
   - Illegal Characters: /*?[]()$!^;'"`~><&|{}

5. In the **Comment** box, type a description for the workflow.

   The maximum number of allowed characters for the **Comment** field is 128.
6. From the **Send Notifications** list, select how to send notifications for the workflow:

   - To use the notification configuration that is defined in the policy resource to specify when to send a notification, select **Set at policy level**.
   - To send notifications with information about each successful and failed workflow and action, after the workflow completes all the actions, select **On Completion**.
   - To send notifications with information about each failed workflow and action, after the workflow completes all the actions, select **On Failure**.

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

   The default notification action is to send the information to the `policy_notifications.log` file. By default, the `policy_notifications.log` file is located in the `/nsr/logs` directory on Linux and in the `C:\Program Files\EMC NetWorker\nsr\logs` folder on Windows.

   Use the default mailer program on Linux to send email messages or the `smtpmail` application on Windows:

- To send notifications to a file, type the following command, where `policy_notifications.log` is the name of the file:

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

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

  ```
  mail -s subject recipient
  ```

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

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

  where:

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

8. In the **Running** section, perform the following steps to specify when and how often the workflow runs:

   a. To ensure that the actions that are contained in the workflow run when the policy or workflow starts, in the **Enabled** box, leave the option selected. To prevent the actions in the workflow from running when the policy or workflow that contains the action starts, clear this option.

   b. To start the workflow at the time that is specified in the **Start time** attribute, on the days that are defined in the action resource, in the **AutoStart Enabled** box, leave the option selected. To prevent the workflow from starting at the time that is specified in the **Start time** attribute, clear this option.

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

   The default value is 9:00 PM.

   d. To specify how frequently to run the actions that are defined in the workflow over a 24-hour period, use the **Interval** attribute spin boxes. If you are performing transaction log backup as part of application-consistent protection, you must specify a value for this attribute in order for incremental transaction log backup of SQL databases to occur.

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

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

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

   For example, if the **Start Time** is 7:00 PM, the **Interval** is 1 hour, and the **Interval End** is 11:00 PM., then the workflow automatically starts every hour beginning at 7:00 PM. and the last start time is 11:00 PM.

9. In the **Groups** group box, specify the protection group to which the workflow applies.

   To use a group, select a protection group from the **Groups** list. To create a protection group, click the **+** button that is located to the right of the **Groups** list.

10. Click **Add**.

    The Policy Action Wizard appears.

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

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

    - Legal Characters: _ : - + = # , . % @
    - Illegal Characters: /*?[]()$!^;'"` ~><&|{}

12. In the **Comment** field, type a description for the action.

13. To ensure that the action runs when the policy or workflow that contains the action is started, in the **Enabled** box, select the option. To prevent the action from running when the policy or workflow that contains the action is started, clear this option.

    > ⓘ Note: When you clear the **Enabled** option, actions that occurs after a disabled action do not start, even if the subsequent options are enabled.

14. From the **Action type** list, select **Clone**.

15. Specify the order of the action in relation to other actions in the workflow:

    - If the action is part of a sequence of actions in a workflow path, in the **Previous** box, select the action that should precede this action.
    - If the action should run concurrently with an action, in the **Previous** box, select the concurrent action, and then select the **Concurrent** checkbox.

16. Specify a weekly, monthly, or reference schedule for the action:

    - To specify a schedule for each day of the week, select **Define** option under **Select Schedule** and period as **Weekly by day**.
    - To specify a schedule for each day of the month, select **Define** option under **Select Schedule** and period as **Monthly by day**.
    - To specify a customized schedule to the action, select **Select** option under **Select Schedule** and choose a customized schedule using the drop down menu that is already created under NSR schedule resource.

17. Specify the days to perform cloning:

    - To clone on a specific day, click the **Execute** icon on the day.
    - To skip a clone on a specific day, click the **Skip** icon on the day.
    - To check connectivity every day, select **Execute** from the list, and then click **Make All**.

    The following table provides details on the icons.

Table 13 Schedule icons

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

18. Click **Next**.

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

19. In the **Data Movement** section, define the volumes and devices to which NetWorker sends the cloned data:

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

    b. In the **Delete source save sets after clone completes** box, select the option to instruct NetWorker to move the data from the source volume to the destination volume after clone operation completes. This is equivalent to staging the save sets.

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

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

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

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

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

       - **Do Not Filter**—NetWorker inspects the save sets in the media database to create a clone save set list that meets the time filter criteria.
       - **Accept**—The clone save set list includes save sets that are saved within the time range and meet all the other defined filter criteria.
       - **Reject**—The clone save set list does not include save sets that are saved within the time range and meet all the other defined filter criteria.

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

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

       ⓘ **Note:** For NAS device, only Snapshot save set is applicable.

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

       - **Do Not Filter**—NetWorker inspects the save sets that are associated with the clients in the media database, to create a clone save set list that meets the client filter criteria.

   - **Accept**—The clone save set list includes eligible save sets for the selected clients.
   - **Reject**—The clone save set list does not include eligible save sets for the selected clients.

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

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

   Note: For NAS device, only full backup level is applicable.

21. Click **Next**.

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

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

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

23. In the **Parallelism** field, specify the maximum number of concurrent operations for the action. This is applicable if multiple rollover is implemented at an action level.

24. From the **Failure Impact** list, specify what to do when a job fails:

    - To continue the workflow when there are job failures, select **Continue**.
    - To abort the current action if there is a failure with one of the jobs, but continue with subsequent actions in the workflow, select **Abort action**.

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

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

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

25. From the **Send Notifications** list box, select whether to send notifications for the action:

    - To use the notification configuration that is defined in the Policy resource to send the notification, select **Set at policy level**.
    - To send a notification on completion of the action, select **On Completion**.
    - To send a notification only if the action fails to complete, select **On Failure**.

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

    The default notification action is to send the information to the `policy_notifications.log` file. By default, the `policy_notifications.log` file is located in the /nsr/logs directory on Linux and in the C:\Program Files\EMC NetWorker\nsr\logs folder on Windows.

Use the default mailer program on Linux to send email messages or the smtpmail application on Windows:

- To send notifications to a file, type the following command, where policy_notifications.log is the name of the file:

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

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

  ```
  mail -s subject recipient
  ```

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

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

  where:

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

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

    To specify the month, use the navigation buttons and the month list box. To specify the year, use the spin boxes. You can set an override in the following ways:

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

      > **Note:**
      > - You can edit or add the rules in the **Override** field.
      > - To remove an override, delete the entry from the **Override** field.
      > - If a schedule is associated to an action, then override option is disabled.

30. Click **Next**.

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

Clone reports

You can use the NMC Reports view to access reports of NetWorker clone operations on a Data Domain system. Generating reports on page 169 provides details.

Monitoring the status of Cloud Tier save sets

The clone flag (clflags) attribute of a save set displays the status of a save set on a Cloud Tier device. A *T* flag appears in the **clflags** attribute for a save set that resides on a Cloud Tier device and does not yet reside in the public cloud. The *T* flag does not appear after the save set is successfully cloned to the public cloud. Use the `mminfo` command and the NMC save sets window to determine the status of save sets on a Cloud Tier device.

Using mminfo to review the status of a save set cloned to a Cloud Tier device

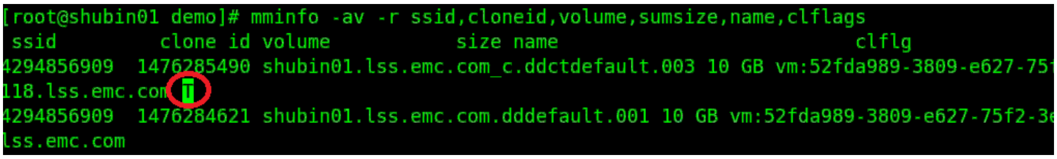
Use the `mminfo` command to display the clone flag status of a save set from a command prompt.

For example, to display the status of a Cloud Tier save set on all Cloud Tier volumes, type the following command:

```
mminfo -av -r ssid,cloneid,volume,sumsize,name,clflags
```

The following figure provides an example of the `mminfo` output for a save set that resides on a Cloud Tier device and does not yet reside in the public cloud.

Figure 50 mminfo output for Cloud Tier save set



```
[root@shubin01 demo]# mminfo -av -r ssid,cloneid,volume,sumsize,name,clflags
 ssid         clone id volume           size name                          clflg
4294856909  1476285490 shubin01.lss.emc.com_c.ddctdefault.003 10 GB vm:52fda989-3809-e627-75f
118.lss.emc.com T
4294856909  1476284621 shubin01.lss.emc.com.dddefault.001 10 GB vm:52fda989-3809-e627-75f2-3e
lss.emc.com
```

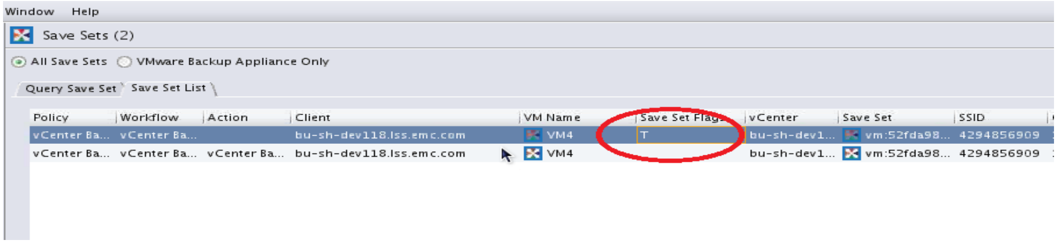
Using NMC to review the status of a save set cloned to a Cloud Tier device

Use the **Save set** window to review the status of save set on a Cloud Tier device. A *T* flag appears in the **Save Set Flags** column for a save set that resides on a Cloud Tier device but does not yet reside in the public cloud.

To review the status of a save set on a Cloud Tier device, perform the following steps:

1. Connect to the NetWorker server by using NMC, and then on the **Administration** window, click **Media**.
2. On the left navigation pane, select **Save Sets**.
3. Click the **Save Set List** tab.
4. (Optional) From the **View** menu, select **Choose Table Columns**, and then select **Save Set Flags**.

Figure 51 Status of Cloud Tier save sets in NMC



Policy	Workflow	Action	Client	VM Name	Save Set Flags	vCenter	Save Set	SSID
vCenter Ba...	vCenter Ba...		bu-sh-dev118.lss.emc.com	VM4	T	bu-sh-dev1...	vm:52fda98...	4294856909
vCenter Ba...	vCenter Ba...	vCenter Ba...	bu-sh-dev118.lss.emc.com	VM4		bu-sh-dev1...	vm:52fda98...	4294856909

The **Save Set Flags** column displays a *T* for a save set that resides on a Cloud Tier device but does not yet reside in the public cloud.

Cloning with nsrclone

Use the `nsrclone` command to configure detailed CCR operations that you can launch by either running the `nsrclone` command manually or by scheduling a task on the operating system or an external scheduler that runs the `nsrclone` command. This method is best for larger environments where flexibility and control of conditions are necessary. Some examples are as follows:

- Start clone job B, which clones to tape storage, if and only if clone job A, which performs CCR, has successfully completed.
- Clone only specific save sets to specified storage nodes or specified devices.
- Perform a CCR from a host other than the NetWorker server or a NetWorker storage node. This command must specify the NetWorker server by its primary hostname. Use the hostname listed in the NMC Enterprise view. Otherwise, the CCR operation may produce normal clones instead.

Scripted solutions require additional knowledge and have external dependencies, such as operating systems and scripting tools, that are beyond the scope of this guide.

The *NetWorker Administration Guide* and the *NetWorker Command Reference Guide* provide more details. Dell EMC Professional Services can also provide assistance.

ⓘ **Note:** When RPS is enabled, each workflow reserves 30 sessions on a target DDBoost device

Staging data from DD Cloud Tier devices

NetWorker supports staging, or moving data to a DD Cloud Tier device from a Data Domain device. NetWorker does not support staging data from a DD Cloud Tier device.

Before you begin

The DD Cloud Tier device that receives the staged data must reside on the same storage unit at the Data Domain device.

About this task

Perform the following steps to stage all the data from a Data Domain device to a DD Cloud Tier device.

ⓘ **Note:** The *NetWorker Administration Guide* provides detailed information about staging.

Procedure

1. In the **Administration** window, click **Devices**.
2. In the left navigation pane, select **Staging**.
3. From the **File** menu, select **New**.

The **Create Staging** dialog box appears, starting with the **General** tab.

4. In the **Name** box, type a name for the staging policy.
5. In the **Comment** attribute, type a description for the staging policy.
6. In the **Enabled** attribute, select **Yes** to enable the staging policy or **No** to disable the staging policy.

   When you select **Yes**, NetWorker automatically starts the staging policy, based on the configuration settings that you define.
7. In the **Devices** attribute, select the check boxes next to each source device from which you want to stage data.

   You can assign multiple devices to a single staging policy. However, you cannot assign a single device to multiple staging policies.
8. In the **Destination pool** attribute, select a DD Cloud Tier pool. For example, DD Cloud Tier Default Clone.
9. In the **Configuration** group box, specify the criteria that starts the staging policy.

   The following table summarizes the available criteria that you can define for the staging policy.

Table 14 Staging criteria options

Option	Configuration steps
High water mark (%) Low water mark (%)	Use these options to start the stage policy based on the amount of used disk space on the file system partition on the source device. You must define a value higher than the value defined in the **Low water mark (%)** attribute. **High water mark (%)**—Defines the upper used disk space limit. When the percentage of used disk space reaches the value that is defined in the **High water mark (%)** attribute, NetWorker starts the stage operation to move save sets from the source disk. **Low water mark (%)**—Defines the lower used disk space limit. When the percentage of used disk space reaches the value that is defined in the Lower water mark (%) attribute, NetWorker stops moving save sets from the source disk. ⓘ Note: When staging and backup operations occur concurrently on the source disk device, NetWorker does not accurately display the disk volume usage total in the Written column in output of the `mminfo -mv` command or in the **Used** column on the **Media** window of the NetWorker Administration application.
Save set selection	Use this option to rank the order in which NetWorker stages the save sets, based on save set size or age. Available values include: • **largest save set**—Stage the save sets in order of largest save set size to smallest save set size. • **oldest save set** —Stage the save sets in order of oldest save set to most recent save set. • **smallest save set**—Stage the save sets in order of smallest save set size to largest save set size.

Table 14 Staging criteria options (continued)

Option	Configuration steps
	• **youngest save set**—Stage the save sets in order of most recent save set to least recent save set.
Max storage period **Max storage period unit**	Use this option to start the stage operation based on the amount of time that a save set has resided on the volume. • **Max storage period**—Defines the number of hours or days that a save set can reside on a volume before the stage process considers the save eligible to move to a different volume. • **Max storage period unit**—Defines the unit of measurement for the value in the max storage period attribute. Available values are Hours and Days. The maximum storage period setting is used along with the file system check interval. Once the maximum storage period is reached, staging does not begin until the next file system check.
Recover space interval **Recover space unit**	Use this option to determine when the stage operation removes the successfully staged save set from the source volume. • **Recover space interval**—Defines the frequency in which NetWorker starts of the recover space operation, which removes successfully stage data from the source volume. • **Recover space unit**—Defines the unit of measurement for the value in the recover space interval attribute. Available values are Hours and Days.
File system check interval	Use this option to define when NetWorker automatically starts the staging process. • **File System Check Interval**—Defines the frequency in which NetWorker starts the staging process. At every file system check interval, if either the high water mark or the maximum storage period has been reached, then staging begins. • **File system check unit**—Defines the unit of measurement for the value in the file system check interval attribute. Available values are Hours and Days.

10. Optionally, to start the staging process immediately:

    a. Select the **Operations** tab.

    b. From the **Start Now** list, select the component of the staging process to perform immediately, for all source devices that are assigned to the staging policy:

    - **Recover space**—To recover space for save sets with no entries in the media database and to delete all recycled save sets.
    - Select **Check file system**—To check the file system and stage eligible sage set data to a destination volume.
    - Select **Stage all save sets**—To stage all save sets to a volume in the destination pool.

    After the staging operation is complete, this option returns to the default setting (blank).

11. Click **OK**.

CHAPTER 5

Restoring Data

This chapter includes the following topics:

Restoring DD Boost deduplicated data

You can restore deduplicated data from DD Boost devices in the same way as you restore non-deduplicated data.

Each backup consists of the following components that reside in different places:

- Deduplicated client backup data resides on the DD Boost devices on the Data Domain system.
- Backup metadata, which specifies how long you want to retain the data and allows you to browse the backups for recovery, resides in the media database and the client file indexes on the NetWorker server.

Restore requirements for deduplicated data

To restore deduplicated data from a DD Boost device, ensure that the following requirements are met:

- All the deduplicated data must be available on the Data Domain system. The retention periods for the backups must not have expired.
- The Data Domain system and the NetWorker storage node must be online during the restore of deduplicated data.

Data recover from DD Cloud Tier devices

Data recoveries from a DD Cloud Tier device requires a mounted Data Domain device on the same storage unit as the DD Cloud Tier device.

When you recover file system data from a DD Cloud Tier device, the recovery process clones the data from the DD Cloud Tier device to a Data Domain device, and then recovers the data from the Data Domain device. NetWorker removes the clone data from the Data Domain device 7 days later.

Before you perform a VMware or BBB recovery of data that resides on a DD Cloud Tier device, review the following information:

- Recovering a full VMware backup from a DD Cloud Tier device is supported.
- Performing a VMware FLR recovery from a DD Cloud Tier device is not supported. To perform a FLR recovery of data that resides only on a DD Cloud Tier device, clone the data to a Data Domain device, and then recover the data from the Data Domain device.
- Performing a Blocked-Based Backup (BBB) FLR recovery from a DD Cloud Tier device is supported.

The *NetWorker VMware Integration Guide* describes how to perform VMware recoveries and the *NetWorker Administration Guide* describes how to perform BBB recoveries.

Supported NetWorker restore procedures

You restore deduplicated data from DD Boost devices in the same way as you restore non-deduplicated data.

- You can select the files or save sets that you want to recover by using NetWorker to browse the client file index.
- You can perform directed restores for supported NetWorker clients and supported NetWorker storage nodes.
- You can try to restore expired backup data by using the NetWorker scanner program to reconstruct a media index from the surviving metadata.

The *NetWorker Administration Guide* provides procedures for data recovery.

Note:
For a Linux client with 2 GB of (RAM), it is recommended that you recover only up to a maximum of 3500 files at a time. If you try to recover more than this limit, an error message similar to the following appears:

```
readv from DD failed for read size 262144: Reading from a file failed
recover: Reading from a file failed [5001] ([31587] [140129876305664] ddp_read()
failed Offset 0, BytesToRead 262144, BytesRead 0 Err: 5001-Unable to allocate file
ddcl buffers rec_create: out of memory.
```

Data Domain Compressed Restore

NetWorker 19.1 and later supports the Data Domain Boost Compressed restore feature for file systems which is enabled by default with packaged Data Domain Boost Library versions 3.5.0.0 and DDOS 6.0.0.30 or later. Data Domain compressed restore is useful in low speed and high latency networks or high speed and highly utilized networks. It helps to achieve greater aggregate throughput because reduced number of bytes are sent over the network. This feature is not applicable for all supported NetWorker clients below 19.2.

Data Domain Boost Compressed restore is also supported for NMM, SQL, VDI, and NMDA modules. Refer to the following guides for more information.

- *Dell EMC NetWorker Module for Microsoft for SQL VDI User Guide*
- *Dell EMC NetWorker Module for SAP Administration Guide*
- *Dell EMC NetWorker Module for Databases and Applications Administration Guide*

Note: Data Domain Boost Compressed restore is not supported for Vproxy restores.

Data Domain Compressed restore can be disabled by creating the file `disable_compressed_restore` at the `/nsr/debug` location.

Restoring by Client Direct over IP from an FC-enabled device

You can use Client Direct over an IP network to restore data from a volume that you have mounted on an FC-enabled DD Boost device. You must share the volume with an IP-enabled device.

Procedure

1. Create an IP-enabled DD Boost device on which to mount the volume. Associate this device with a different storage node than the one that manages the FC-enabled DD Boost device.

   The storage node that you use for the IP restore must not have an FC-enabled DD Boost device available to the volume.

   Configuring DD Boost devices with the NMC Device Configuration wizard on page 59 provides details.

2. Configure the devices to share the volume.

   Configuring volume sharing on multiple devices on page 92 provides details.

3. Modify the Client resource for the client that will receive the restored data.

   - Configure this client for Client Direct and IP connectivity.
   - On the **Globals (2 of 2)** tab, in the **Recovery storage nodes** field, specify the storage node that you associated with the IP-enabled DD Boost device.

     Note: This option is now only available in the Diagnostic Mode view.

     Configuring a backup client with NMC property windows provides details.

4. Mount the volume on the new IP-enabled DD Boost device and perform the restore by using the new IP-restore Client resource.

Disaster recovery

A disaster is defined as the loss of data where the computing environment required to restore that data is not available. Disaster recovery is necessary when ordinary data recovery procedures are not sufficient to recover the computing environment and its data to normal day-to-day operations.

Causes of disaster

A disaster can result from any of the following situations:

- Debilitating hardware or software failures
- Computer viruses that corrupt the computing system
- Infrastructure interruptions, inconsistencies, or loss of services, such as problems with communications or network connections that result in damage to the computing environment

Potential losses

Disaster recovery of the primary site must cover the potential loss of one of more of the following systems at the primary site:

- The Data Domain server that stores the deduplicated client backups
- The NetWorker storage node that stores the deduplication metadata for the backups
- The NetWorker server that stores the metadata for the backups in the media database and client file indexes

Disaster recovery requirements

A complete disaster recovery environment provides a secondary site with systems that copy all the information that is involved in each completed backup that is performed at the primary site.

You can configure the primary site and the secondary site to provide disaster recovery for each other, with each serving as both a primary site, and secondary site with different datazones for different clients.

Disaster recovery requires the maintenance of the following systems:

- Data Domain system with deduplicated client data that is cloned from the primary Data Domain system
- Disaster recovery NetWorker storage node with deduplication metadata that is cloned from the primary NetWorker storage node
- Disaster recovery NetWorker server with metadata that is cloned from the primary NetWorker server

Disaster recovery environment on page 38 shows an example of a simple disaster recovery environment.

Disaster recovery scenarios

The procedures that you use to recover from a disaster varies depending on the circumstances, which could include the following factors:

- The deployment of the disaster recovery environment

- Which systems are affected by the disaster
- The time that is required to successfully recover from the disaster

The *NetWorker Server Disaster Recovery and Availability Best Practices Guide* provides details.

Bootstrap recovery from a DD Cloud Tier device

NetWorker does not support recovering a bootstrap backup from a DD Cloud Tier device directly.

To recover data from a bootstrap backup that resides on a DD Cloud Tier device, you must clone the data from the DD Cloud Tier device to a Data Domain device that is on the same Data Domain system and storage unit as the DD Cloud Tier device.

The *NetWorker Administration Guide* provides detailed information about how to perform a disaster recovery of a NetWorker server when the bootstrap resides on a DD Cloud Tier device.

CHAPTER 6

Monitoring, Reporting, and Troubleshooting

This chapter includes the following topics:

Monitoring Data Domain events, statistics, and logs

The NetWorker Management Console (NMC) provides several ways to view the backup statistics, the logs, and the events for connected Data Domain systems.

Viewing the statistics, logs, and alerts

When you use the NetWorker Management Console (NMC) to connect to the NetWorker server, the NetWorker Administration window provides a comprehensive view of the backup status, logs, and alerts for connected Data Domain systems.

About this task

> **Note:** In some logs and notifications, the Administration window lists Client Direct operations variously as direct file assess (DFA), direct file save, or DIRECT_FILE operations.

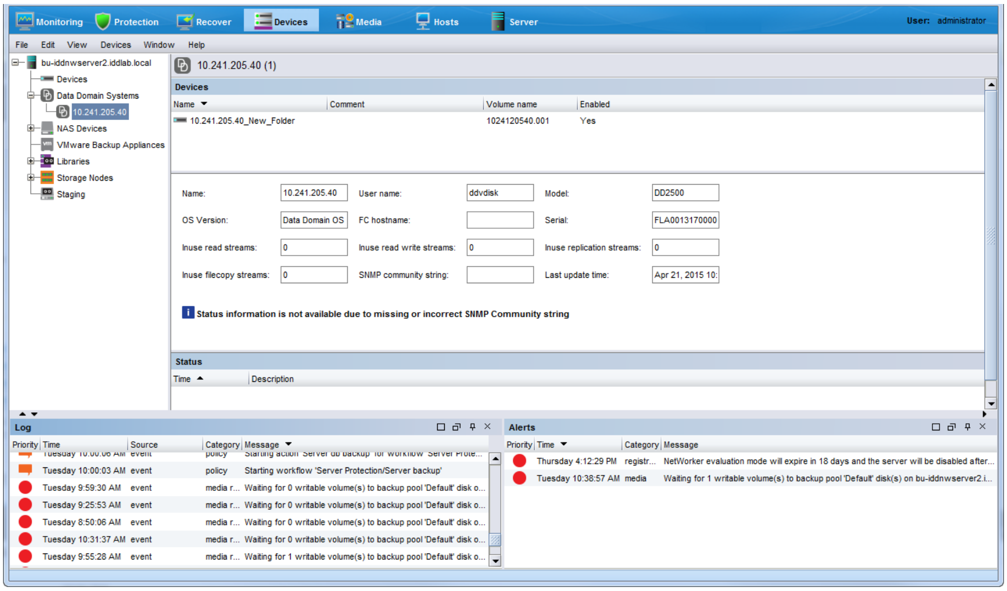
Procedure

1. Ensure that you have configured SNMP for the Data Domain system.

   Configuring SNMP for an NMC managed Data Domain system on page 168 provides details.

2. In the Administration window, click the **Devices** view.
3. In the folder tree, expand **Data Domain Systems**, and perform one of the following actions:
   - Right-click a Data Domain system, and select **Properties** to view system information, including the identity (name, hosts, model, OS version, serial number), configuration, SNMP community string, access credentials, capacity status information, save stream status information, and system details.
   - To view backup information select a Data Domain system, as shown in the following figure.

Figure 52 NetWorker Administration window displaying DD Boost devices



Devices

Name	Comment	Volume name	Enabled
10.241.205.40_New_Folder		1024120540.001	Yes

Name: 10.241.205.40
User name: ddvdisk
Model: DD2500
OS Version: Data Domain OS
FC hostname:
Serial: FLA0013170000
Inuse read streams: 0
Inuse read write streams: 0
Inuse replication streams: 0
Inuse filecopy streams: 0
SNMP community string:
Last update time: Apr 21, 2015 10:

Status information is not available due to missing or incorrect SNMP Community string

Status

Time	Description

Log

Priority	Time	Source	Category	Message
	Tuesday 10:00:06 AM	event	policy	Starting action 'Server db backup' for workflow 'Server Prote...
	Tuesday 10:00:03 AM	event	policy	Starting workflow 'Server Protection/Server backup'
●	Tuesday 9:59:30 AM	event	media r...	Waiting for 0 writable volume(s) to backup pool 'Default' disk o...
●	Tuesday 9:25:53 AM	event	media r...	Waiting for 0 writable volume(s) to backup pool 'Default' disk o...
●	Tuesday 8:50:06 AM	event	media r...	Waiting for 0 writable volume(s) to backup pool 'Default' disk o...
●	Tuesday 10:31:37 AM	event	media r...	Waiting for 0 writable volume(s) to backup pool 'Default' disk o...
●	Tuesday 9:55:28 AM	event	media r...	Waiting for 1 writable volume(s) to backup pool 'Default' disk o...

Alerts

Priority	Time	Category	Message
●	Thursday 4:12:29 PM	registr...	NetWorker evaluation mode will expire in 18 days and the server will be disabled after...
●	Tuesday 10:38:57 AM	media	Waiting for 1 writable volume(s) to backup pool 'Default' disk(s) on bu-iddnwserver2.i...

- The **Devices** area shows the following device and usage information:

- Pre-Compression—If the data had not been deduplicated and compressed, indicates the amount of space that the backup would have used. NetWorker tracks this value as the size of backups.
- Compression (Reduction)—Represents the data compression with the pre-compression and post-compression used values. Data compression is calculated with:
  [(1 - Post-comp Used) ÷ Pre-Compression] x 100%
- /backup: post-comp—Indicates the total capacity of the Data Domain system, the amount of disk space already in use, and the amount of space that is available.
- /ddvar—Indicates the amount of log file space that is in use on the Data Domain file system.

- The **Status** area lists the connectivity usage.
- The **Log** table shows a chronological list of events that occur during NetWorker server operations.
- The **Alerts** table lists the messages for operational issues that can require administrative attention. Data Domain alerts are available only if SNMP traps are configured.

  ⓘ Note: To delete individual messages from the **Alerts** table, open the NMC **Events** view, select the messages, right-click, and select **Dismiss**.

Viewing backup statistics in NMC

You can view the storage statistics for backups on a connected Data Domain system.

About this task

In the **NMC Enterprise** view, select a Data Domain host. A table shows the backup statistics for the selected system.

Viewing backup alerts (SNMP traps) in NMC

Alerts are messages that appear for operational issues, that can require administrative attention.

About this task

You can view backup alerts for a connected Data Domain system.

Procedure

1. Configure SNMP for the Data Domain system.

   Configuring SNMP for Data Domain provides details.

2. In NMC, select the **Events** view.

   A table lists the backup alerts (SNMP traps) in chronological order.

   ⓘ Note: The same alert messages also appear in the NetWorker **Alerts** table.

Deleting individual messages

You can delete individual messages from the NetWorker Alerts table and the NetWorker Management Console (NMC) Events table by removing the messages from the NMC Events table. Both views show the same messages.

Procedure

1. In NMC, select the **Events** view.
2. In the Events table, select the messages that you want to remove.
3. Right-click and select **Dismiss**.

   NSM deletes the selected messages.

Configuring SNMP for an NMC managed Data Domain system

You can configure the NetWorker Management Console (NMC) to monitor Data Domain alerts (SNMP traps) when you add a Data Domain system to the NMC Enterprise. You can also update an existing Data Domain system that is managed by the NMC server. If you have viewing privileges, in the NetWorker Management Console (NMC) Enterprise view you can view a list of the Data Domain systems as network hosts.

About this task

Adding a host Data Domain system to NMC Enterprise view describes how to add a Data Domain system to the NMC Enterprise view.

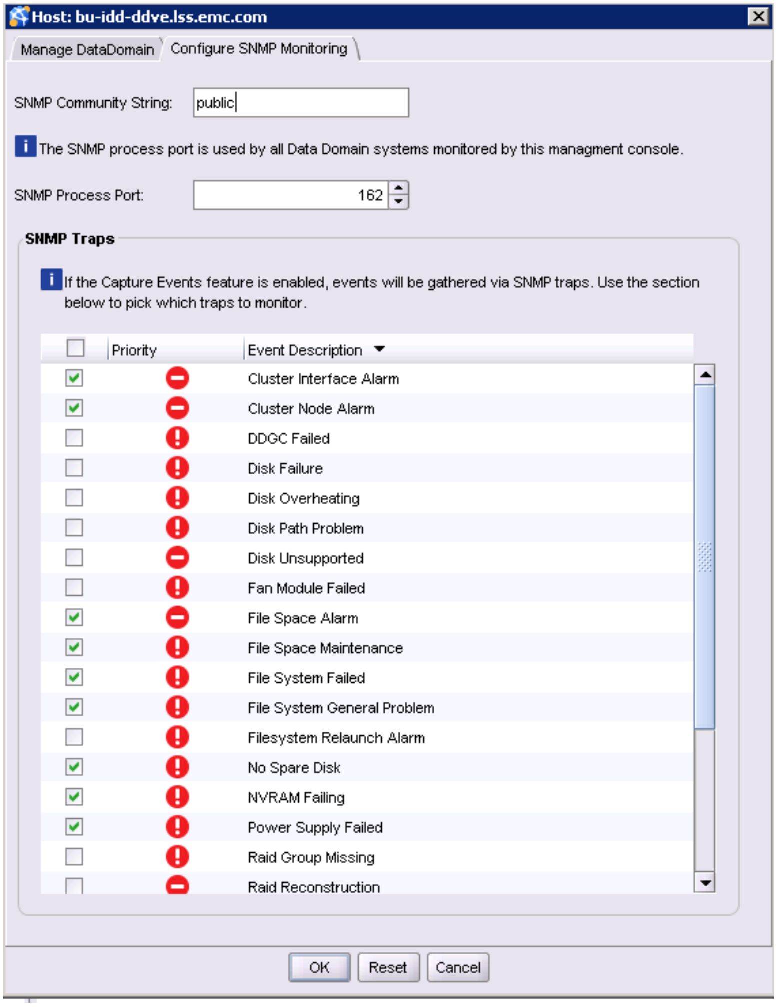
Procedure

1. Enable SNMP on the Data Domain system and configure the system to send traps to the NMC server. Configuring the Data Domain system for DD Boost provides details.
2. In the NMC **Enterprise** view, in the left panel, right-click the Data Domain system that you want to monitor, and select **Properties**.
3. In the **Properties** window, on the **Manage Data Domain** tab, ensure that **Capture Events** is enabled.

   If you do not select the **Capture Events** checkbox, NMC monitors the status of the DD Boost devices but will not monitor the Data Domain SNMP traps that are required to monitor events.

4. On the **Configure SNMP monitoring** tab, type a value for **SNMP Community String**. The typical setting is `public`, which allows all users to monitor events.
5. In the **SNMP Process Port** field, type a value for the port that the Data Domain system uses for SNMP traps. Firewall requirements provides details.
6. In the **SNMP Traps** section, select the SNMP traps that you want to monitor. Some traps are pre-selected. The following figure shows an example for Data Domain 5 alerts. Other versions might differ.

Figure 53 Data Domain alerts to monitor



SNMP Community String: public

The SNMP process port is used by all Data Domain systems monitored by this managment console.

SNMP Process Port: 162

SNMP Traps

If the Capture Events feature is enabled, events will be gathered via SNMP traps. Use the section below to pick which traps to monitor.

□	Priority	Event Description
☑	⛔	Cluster Interface Alarm
☑	⛔	Cluster Node Alarm
□	❗	DDGC Failed
□	❗	Disk Failure
□	❗	Disk Overheating
□	❗	Disk Path Problem
□	⛔	Disk Unsupported
□	❗	Fan Module Failed
☑	⛔	File Space Alarm
☑	❗	File Space Maintenance
☑	❗	File System Failed
☑	❗	File System General Problem
□	❗	Filesystem Relaunch Alarm
☑	❗	No Spare Disk
☑	❗	NVRAM Failing
☑	❗	Power Supply Failed
□	❗	Raid Group Missing
□	⛔	Raid Reconstruction

7. Click **OK**.

Generating reports

You can use the NetWorker Management Console (NMC) Reports view to create statistical reports of NetWorker with Data Domain backup, recovery, and cloning activities.

Configuring a report

You can configure and display a Data Domain report for backup or clone activities in the NetWorker Management Console (NMC).

Procedure

1. In the **NetWorker Management Console** window, click **Reports**.
2. Expand the **Reports** folder, expand the **Legacy Reports** folder, and then the **Data Domain Statistics** folder. Select the report that you want to view.

   ⓘ **Note:** The types of reports include summary, statement, and details.

   The Configure tab for the selected report type appears in the right panel.

3. In the Configure tab, configure the items that you want to include in the report. Select the item parameters and click the **Remove**, **Add**, **Remove All** , or **Add All** buttons as required. The specific parameters that are available depend on the type of report that you select.

   If you do not specify Save Time values, the report displays all the available data. The following table lists details of report configuration parameters.

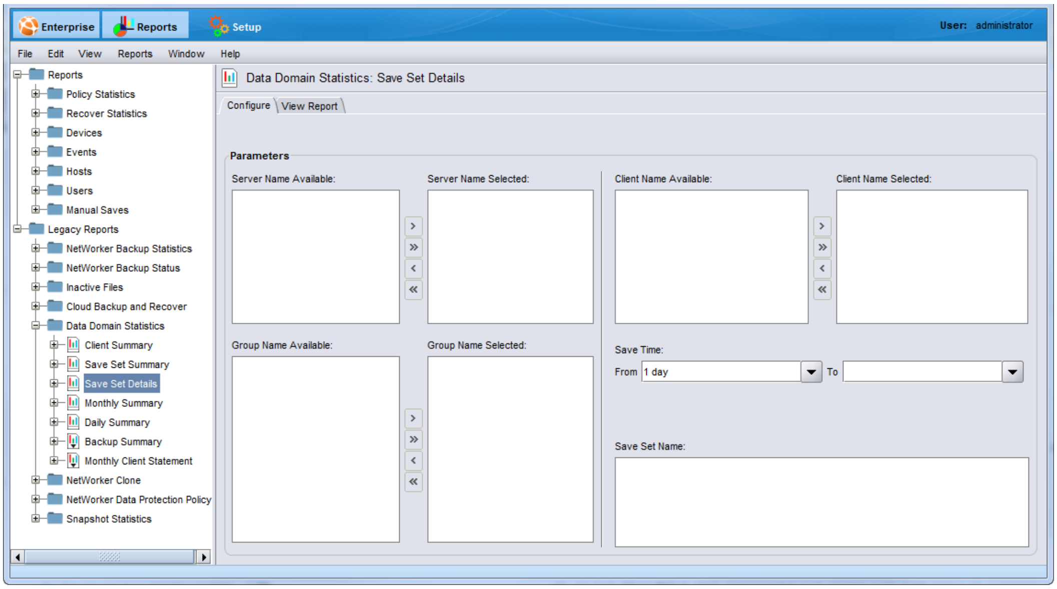
   Table 15 Data Domain report configuration parameters

Parameter	Description	Options
Server Name	Specifies managed hosts within the enterprise.	Selected server names
Group Name	Selects one or more groups.	Selected group names
Client Name	Specifies one or more clients. ⓘ Note: Monthly report does not include the Client Name parameter.	Selected client names
Save Set Name	Specifies one or more save sets. Values are case-sensitive and you cannot use wildcard characters. ⓘ Note: Monthly report does not include the Save Set Name parameter.	Selected save set names
Save Time	Limits the report to a specified time range. The date/time format available depends on the language locale of the operating system.	Save time (within a range)

   The following figure shows an example report configuration.

4. To display the report, select the **View Report** tab.

Figure 54 Report configuration



Types of backup reports

Backup reports are available in the following formats:

- Basic reports on page 171 describes details of basic reports.
- Drill-down reports describes details of drill-down reports.
- Advanced reporting on page 173 describes advanced reporting functionality with the optional Data Protection Advisor (DPA).
-

For clone operations, no specific reports are available. You can query and list the copies of save sets in the NetWorker Administration, Media view, under Save Sets.

Basic reports

A basic report displays statistics for a specific datazone component, a time span, or a field. You can view reports within the NetWorker Management Console (NMC) Enterprise **Reports** window, and also modify the scope of a basic report by adjusting the parameters.

The following table describes the basic reports that are available for Data Domain statistics.

Table 16 Data Domain basic reports

Report name	Purpose
Client Summary	For all or specified clients, displays the following statistics: • Amount of data—Amount of the data that NetWorker would have moved by using a conventional backup (protected data). • Target size—Size of the data after deduplication has taken place on the Data Domain system (stored data). • Deduplication ratio—Percentage of savings by using Data Domain deduplication.

Table 16 Data Domain basic reports (continued)

Report name	Purpose
	• Number of save sets—The number of save sets in the backup. • Number of files—The number of files in the backup.
Save Set Summary	For all or specified save sets, displays the following deduplication statistics: • Amount of data—Amount of the data that NetWorker would have moved by using a conventional backup. • Target size—Size of the data after deduplication has taken place on the Data Domain system. • Deduplication ratio—Percentage of disk space that is saved by using deduplication. • Number of save sets—Number of save sets in the backup. • Number of files—Number of files in the save set.
Save Set Details	Displays details about each save set, including backup duration and the following statistics: • Server Name • Save Set Name and ID • DD Retention Lock Type • DD Retention Locked Till • Action Type • Policy Name • Workflow and Workflow Start Time • Status • Save Set size—Protected data size • Target size—Size of the data after deduplication has taken place on the Data Domain system (stored data size). • Deduplication ratio—Percentage of savings by using deduplication. • Number of files—Number of files in the save set.
Monthly Summary	Displays statistics on a month-to-month basis.
Daily Summary	Displays statistics on a day-to-day basis.

Drill-down reports

A drill-down report consists of multiple basic reports, which are connected as layers and all configured with the same parameters that the top layer uses.

You can run reports for groups, clients, or save sets. You can view reports within the NetWorker Management Console (NMC) Enterprise **Reports** window, and also modify the scope of a report by adjusting the parameters.

The following table lists the drill-down reports that are available for Data Domain statistics.

Table 17 Data Domain statistics drill-down reports

Report name	Purpose	Sequence
Backup Summary	Reports backup statistics over a period of time, including a client summary.	1. Client Summary 2. Save Set Summary 3. Save Set Details
Monthly Client Statement	Reports backup statistics of individual clients on a month-to-month and day-to-day basis, down to individual save sets details.	1. Client Summary 2. Monthly Summary 3. Daily Summary 4. Save Set Details

Data Domain statistic reports

You can run the Data Domain `gstclreport` command with a specified format to generate a specific Data Domain statistics report.

The Data Domain product documentation provides details.

Advanced reporting

The NetWorker Management Console (NMC) provides reports for only the recent backup history in a specific datazone. The optional Data Protection Advisor (DPA) software can provide extended reports of backups, trends, and analysis for one or multiple datazones, including reports of Data Domain systems. DPA is best for larger environments where you require additional analysis with forecasts and trends.

Replacing a failed or old storage node

Before you begin

Ensure that the following requirements are met:

- The replacement storage node has access to the original Data Domain system.
- The NetWorker server software is the same version as the original.
- The NetWorker server has all the same indexes and the same media database entries as before the disruption.

About this task

If a storage node fails or if you replace a storage node, you can recover the data that is stored on the associated DD Boost devices on the replacement storage node or on a different storage node. The success of the recovery depends on the state of the devices at the time of the loss:

- If the storage volumes were unmounted when the disruption occurred, the structure and integrity of the data remains intact and you can expect a complete recovery.
- If the storage volumes were mounted but not reading or writing data during the disruption, then a complete recovery is likely.
- If the devices were reading or writing at the time of the disruption, then data loss or data corruption is likely to have occurred, and you cannot expect a complete recovery.
  If the volume structure is intact, then the NetWorker server can continue to perform its operations with the existing devices, with minimal impact.

If the replacement storage node has a different name or if you use the NetWorker server as the storage node, then you must re-create the devices in NetWorker as follows.

Procedure

1. Use NMC to connect to the NetWorker server. In the **NetWorker Administration** window, select the **Devices** view, and then select **Devices** in the left navigation pane.
2. For each affected original remote storage node-based DD Boost device, right-click the device, select **Properties**. Record the following information:
   - On the **General** tab:
     - Name
     - Device Access Information
   - On the **Operations** tab:
     - Volume Name
     - Volume Pool
3. Remove the original DD Boost devices from the NetWorker application. The device folders continue to exist on the Data Domain system.

   a. In the **Devices** view, from the **Devices** tree, right-click and unmount each affected device. Mounted devices have a **Volume Name**.

   b. In the **Media** view, from the **Media Pool** tree, right-click each affected media pool (**Volume Pool**), select **Properties**, and on the **Selection Criteria** tab, remove each affected device from the **Target Devices** list.

   c. In the **Devices** view, from the **Devices** tree, right-click and delete each affected device.
4. Re-create the devices on the NetWorker application that is associated with a replacement storage node.

   a. In the **Devices** view, right-click the **Data Domain systems** tree, and then start the **New Device Wizard**.

   b. To access the system, specify the Data Domain system and DD Boost (OST) credentials.

   c. On the **Select Folders to use as Devices** page, select the DD Boost devices (device folders) that are associated with the failed storage node.

   When you leave this page, a message notifies you that NetWorker previously associated the devices with a different storage node. Confirm the selection.

   d. On the **Configure Pool Information** page, specify the media pool for the devices, and clear the **Label and Mount** selection. You must manually mount the devices on the new storage node later in this procedure.

   ⓘ NOTICE If you enable **Label** and **Mount** at this point, NetWorker relabels the volume and you lose all the data. You cannot undo this action.

   e. On the **Select the Storage Nodes** page, select a storage node to handle the new devices by doing one of the following.

   - Select an existing storage node.
   - Create a replacement storage node.
   - Use the NetWorker server’s storage node.
     The storage node must be running on the correct network and its hostname must be resolvable by DNS.

f. Complete the wizard.

5. Manually mount each new device.

   a. In the NMC window for the NetWorker server, click **Devices**.

   b. In the navigation tree, select the Data Domain system.

   c. In the right panel, right-click each device that you want to mount, and select **Mount**.

      The device mounts on the storage node and uses the label that is associated with the pool you specified.

6. Review the NMC log for any error messages.

Results

If this procedure does not report any errors, then the device and the volume are available for use. Backup and recovery operations may require further configuration depending on the original settings and the purpose of the device recovery.

Troubleshooting

The following sections will help you identify and resolve common issues of configuration and operation.

Data Domain system log files

This section provides a list of log files that can assist you in troubleshooting issues that occur when performing operations with Data Domain devices and DD Cloud Tier devices.

Support Bundles

The Data Domain system provides a mechanism to create a Support Bundle, which is a zipped file that contains a number of log files that Support uses to troubleshoot issues.

You can create a Support Bundle by using Data Domain System Manager, or from the system console:

- Data Domain System Manager—Browse to **Maintenance** > **Support** > **Support Bundles** > **Generate Support Bundle**. To download the bundle, click the `GZ` file, and then select **Save**.
- CLI—Log in to the Data Domain system console as the sysadmin user, and then type the following command:

  ```
  support bundle create default
  ```

  Output similar to the following appears:

  ```
  Compressing files...
  Bundle created...
  sysadmin@bu-dd3# support bundle list
  File Upload Size Time Created
  Status (KiB)
  --------------------------------------- ------ -----
  ------------------------
  bu-dd3-support-bundle-1130095714.tar.gz 68440 Wed Nov 30 09:57:14
  2016
  --------------------------------------- ------ -----
  ------------------------
  ```

Core dumps

The Data Domain system generates core dump files that provide detailed information about process crashes.

To display a list of core dumps on the Data Domain system, log in to the Data Domain system console as the sysadmin user, and then type the following command: **`support coredump list`**

Accessing Support Bundles and core dumps from a remote host

Use an NFS client to access Support Bundles and core dump files from a remote host, and to transfer the files to a remote host.

Perform the following steps to access the Support Bundle or core dumps by using an NFS client:

1. On the Data Domain system:
   a. To enable NFS, type: **`enable NFS`**
   b. To provide NFS clients access to the Data Domain system, type: **`nfs add /ddvar *`**
2. On the NFS client:
   a. Create a local folder, by typing: **`mkdir/nfsshare`**
   b. Mount the NFS share on the Data Domain system to the `nfsshare` folder by typing: **`sudo mount`** ***`data_domain_system`*****`:/ddvar/nfsshare`**
   where *data_domain_system* is the hostname or IP address of the Data Domain system.
   c. Change to the directory `/nfsshare/support`
   d. Type the `ls` command to display a list of Support Bundles on the Data Domain system.
   e. Use the `cp` command to copy the files from the `/nfsshare/support` directory to a location on the NFS client.

Troubleshooting DD Cloud Tier data movement issues

Data moves from the DD Cloud Tier to the Cloud Provider at the date and time defined by the data movement policy on the Data Domain system, or when a user manually runs the data movement command. You cannot move data from a DD Active Tier device to the Cloud Provider, you can only move data that you cloned to a DD Cloud Tier device.

When data resides on a DD Cloud Tier device, NetWorker updates the **clflags** attribute for save set with a **T** (in transit) flag. NetWorker clears the **T** flag within 30 minutes of the completion of the data movement operation, and the data is on the Cloud Service Provider.

To view the status of a save set, use the `mminfo` command.

For example, the following output displays a list of save sets that reside on two volumes:

- DDVEbushdev111.001 contains backup data on a Data Domain device
- nw_w2k8_c.ddctdefault.001 contains a clone copy of the save sets on the DDVEbushdev111.001. The data movement operation has not started on these save set yet, or the data movement operation is in progress but the data has not completely moved to the Cloud Provider.

```
mminfo -q"savetime>11/27/2016" -
r"volume,savetime,totalsize,level,name,ssid,clflags"
```

```
volume date total lvl name ssid clflg
DDVEbushdev111.001 11/28/2016 4 full <1>E:\dd 4198279169
DDVEbushdev111.001 11/28/2016 4 full <2>E:\dd 4215056363
DDVEbushdev111.001 11/28/2016 4 full <3>E:\dd 4231833564
DDVEbushdev111.001 11/28/2016 6768 full E:\dd 4181501966
```

```
nw_w2k8_c.ddctdefault.001 11/28/2016 4 full <1>E:\dd 4198279169 T
nw_w2k8_c.ddctdefault.001 11/28/2016 4 full <2>E:\dd 4215056363 T
nw_w2k8_c.ddctdefault.001 11/28/2016 4 full <3>E:\dd 4231833564 T
nw_w2k8_c.ddctdefault.001 11/28/2016 6768 full E:\dd 4181501966 T
```

To determine when the data will move from the DD Cloud Tier device or troubleshoot why the data movement operation has not completed, perform the following steps as the sysadmin user on the Data Domain system:

1. Determine the data movement schedule, by typing the following command:

   ```
   data-movement schedule show
   ```

   For example, output similar to the following appears:

   ```
   Mtree Target(Tier/Unit Name) Policy Value
   ------------------- ---------------------- ----------- -------
   /data/col1/data01 Cloud/common_ecs app-managed enabled
   /data/col1/networker Cloud/common_ecs app-managed enabled
   ------------------- ---------------------- ----------- -------
   ```

   Note: Each mtree can have only one data movement policy.

2. Determine when the status of the last data movement operation, by typing the following command:

   ```
   data-movement status
   ```

3. Determine the data movement schedule, by typing the following command:

   ```
   data-movement policy show
   ```

   Output similar to the following appears:

   ```
   Data-momvement is scheduled to run on day(s) "thu" at "23:00" hrs
   every "2" week(s).
   ```

4. Manually start a data movement operation, by typing the following command:

   ```
   data-movement start mtreesmtree-list
   ```

   For example, to start the operation on mtree `/data/col1/networker`, type:

   ```
   data-movement start trees /data/col1/networker
   Data-movement started
   ```

5. Display real-time status of a data movement operation, by typing the following command:

   ```
   data-movement watch
   ```

   The following output displays the status of a data movement operation that successfully moves 4 files:

   ```
   Data-movement: phase 1 of 3 (copying)
   100% complete; time: phase 0:02:20, total 0:02:31
   Copied (post-comp): None, (pre-comp): 6.63 KiB,
   Files copied: 4, Files verified: 0, Files installed: 0
   Data-movement: phase 2 of 3 (verifying)
   100% complete; time: phase 0:00:02, total 0:02:41
   Copied (post-comp): None, (pre-comp): 6.63 KiB,
   ```

```
Files copied: 4, Files verified: 0, Files installed: 0
Data-movement: phase 3 of 3 (installing files)
100% complete; time: phase 0:00:31, total 0:03:21
Copied (post-comp): None, (pre-comp): 6.63 KiB,
Files copied: 4, Files verified: 0, Files installed: 0
Data-movement was started on Nov 28 2016 15:08 and completed on Nov
28 2016 15:11
Copied (post-comp): None, (pre-comp): 6.63 KiB,
Files copied: 4, Files verified: 4, Files installed: 4
```

> **Note:** If the `data-movement watch` command displays the following line: `Files copied: 0, Files verified: 0, Files installed: 0.`, then the operation did not move any files. This can happen for one of the following reasons:
>
> - The DD Cloud Tier devices does not contain data that is eligible for movement. In this case, confirm that you cloned data to the DD Cloud Tier device.
> - Cloud connectivity issues or other issues exist.

6. Display system alerts that might indicate why a data movement operation failed to copy files, by typing the following command:

   `alert show current`

   Data Domain system log files on page 175 provide more information about the logs files to review to troubleshoot error messages.

Too many streams

NetWorker provides queries the underlying Data Domain to determine the maximum number of data streams the Data Domain system supports and throttles the maximum client sessions and streams to prevent performance degradation on the Data Domain system.

When a NetWorker client requests a session to perform a save, recover, or proxy cloning (NetWorker Clone Controlled Replication) operation on a Data Domain system, the NetWorker server will reject the request if the total number of active data sessions on the Data Domain system exceeds the maximum number of supported streams.

When the NetWorker server rejects the session request, error messages similar to the following appear in the `daemon.raw` file on the NetWorker server:

- Too many save streams (*number*) on DDR *DD_hostname* since that would cause the device to exceed the maximum DDR write stream counts (*max_number*).
- Too many proxy recover streams (*number*) on DDR *DD_hostname* since that would cause the device to exceed the maximum DDR repl read stream counts (*max_number*)
- current_read_stream (%d) reach max_read_stream %d for DDR *DD_hostname*
- Too many recover streams (*number*) on DDR *DD_hostname*' since that would cause the device to exceed the maximum DDR read stream counts (*max_number*)

The NetWorker client will retry the request up to the number of times that is defined by the **Retries** value of the Action resource. The time in between each retry is determined by the value defined in the **Retry Delay** attribute of the Action resource.

Name resolution issues

If connectivity issues are present, ensure that the network names are valid and consistent for the NetWorker server, the storage nodes, and the Data Domain systems. Use the same names that are consistent with the NetWorker software configuration.

Validate the connections from the Data Domain system and the NetWorker server, and from the NetWorker server to the Data Domain system by using the IP addresses and the network names. If you use aliases or short names in the configuration, then verify the aliases and short names. To validate connections, use one of the following methods:

- On the NetWorker server and storage nodes, run the `nslookup` command to verify that network names resolve to the correct IP address.
- On the Data Domain system, run the `net hosts` command.
  Host naming guidelines provides suggestions for names.

Correct any improper names by modifying the DNS entries or by populating the local hosts files.

Network connection issues

You can test the network connections for a Data Domain system by running the `net lookup` command through an SSH Telnet session, which requires administrator or system administrator permissions.

The Data Domain system can also show the current network configuration. Run the `net show` and the other network related commands, available through the Data Domain interface. Log in and go to the specific Data Domain system. Then select the **Hardware** > **Network** tabs to access the commands.

It is recommended that you diagram and verify all relevant network connections. A typical Data Domain network configuration provides a minimum of two network connections, one dedicated to administration and the other to backup data only. You can use 10 GbE connectivity, or multiple backup connections that you can aggregate or team together by running the `ifgroup` command on the Data Domain system.

Network requirements on page 27 provides suggestions for network connections.

Device access errors

Error messages can occur when the NetWorker Management Console (NMC) cannot connect to a Data Domain Boost device.

Volume unavailable error

This message appears when the Data Domain file system becomes inaccessible or disabled, and then you reenable the file system. For example, for service or testing, you could leave the devices in an unmounted state.

Backup operations for the devices will not start and an error message similar to the following appears in the Log pane in the **Administration** window, and the `daemon.raw` file:

```
Waiting for 1 writeable volume(s) to backup pool
```

To resolve this issue mount and enable the device.

1. In the **NetWorker Administration** window, click the **Devices** view.
2. In the **Devices** table, right-click and select **Mount** for any unmounted DD Boost device.

3. To enable the device, in the **Enabled** column, right-click the device, and select **Enable/ Disable**.

NFS service errors

You must enable Data Domain NFS service for the NetWorker software to access DD Boost devices.

Without NFS enabled, an error message similar to the following appears, typically when NetWorker tries to label a device:

```
Failed to contact the Data Domain system. Host could be unreachable, or
username/password could be incorrect. Do you wish to configure manually?
The user has insufficient privilege
```

Configuring the Data Domain system for DD Boost describes how to enable NFS access.

Backup fails for older NetWorker application modules

Some older NetWorker application modules do not support the NetWorker Client resource fields for Data Domain Backup and Target Pool or Pool and you must not use these fields for DD Boost backups. In the **Data Domain Backup** field you specify that backups use only DD Boost devices, even if the configured pool contains other device types, although pools with mixed devices is not a good practice.

The *NetWorker Administration Guide* provides details on how to configure a pool to target only DD Boost devices.

The release notes for the specific NetWorker application modules provide details on supported Data Domain configurations.

Multiple recovery fails on AIX clients with less than 2 GB RAM

For NetWorker clients on AIX systems with less than 2 GB of RAM, a recovery that uses four or more parallel recovery save stream IDs might fail, and an error message similar to the following appears:

```
93124:recover: readv from DD failed for read size 262144: Reading from a file
failed ([5001] memory no longer available)
```

To avoid this error, export the following environment variable on the client shell.

```
LDR_CNTRL=MAXDATA=0x70000000
```

Backing up streams from NetWorker to Apollo DD is rejected

Issue

When you perform a backup of 1024 streams from a NetWorker server to Apollo DD, the backup succeeds. However, if you run three NetWorker servers simultaneously with 3000+ save sets, the system is unable to reach the 1885 write streams limit on Apollo DD. Approximately 1600 write streams start on Apollo DD from the three NetWorker servers, and the system displays connection rejection messages in the `ddfs.info` log file on Apollo DD.

Workaround

To resolve this issue, ensure that you are in SE Mode, then change the attribute NFS_TOTAL_CONNS_PERCENT from the default 50 to 100.

```
reg set system.NFS_TOTAL_CONNS_PERCENT = 100
```

APPENDIX

DD Boost Conversion and Upgrade

This appendix includes the following topics:

Converting DD Boost devices from IP to FC connectivity

After you ensure that the FC support requirements are met, you can convert existing DD Boost devices that use Ethernet IP connections to use FC connections that are deployed as a SAN. No data is lost by the conversion and full DD Boost features are retained, including Client Direct operations for backup and restore.

About this task

Plan the device conversion with the following road map that outlines the sequence of basic tasks that you must perform.

Procedure

1. Ensure that all FC support requirements are met.

   FC support provides details.

2. Configure the **Fibre Channel Options** of the DD Boost devices.

   Configuring DD Boost devices with NMC property windows provides details.

3. Configure the **Data Domain Interface** field of the NetWorker clients for FC.

   Configuring a backup client with NMC property windows provides details.

Redirecting backups from other devices to DD Boost

You can redirect the backups of existing NetWorker clients that do not use DD Boost devices to use new DD Boost devices.

About this task

To redirect the backups, you must configure the Pool resource to use DD Boost devices.

After you redirect backups to DD Boost devices, you must perform a full backup of the data. This practice avoids a dependency on the last full backup in the legacy storage environment and the potential need to restore from two different environments. Do one of the following to perform a full backup after you configure a DD Boost Pool resource:

- Configure the redirection of the backups to a DD Boost device at a time when the next scheduled backup for the client data is a full backup.
- Configure the redirection, and then change the backup schedule to accommodate an initial full backup.

To use storage on DD Boost devices, complete the following steps to redirect data from existing scheduled client backups.

Procedure

1. Ensure that the required network connection, hostname resolutions, and licenses are available and ready to use. The following sections provide details:

   - Licensing in Data Domain systems
   - Host naming guidelines
   - Network requirements on page 27

2. Configure the Data Domain system for use with NetWorker. Configuring the Data Domain system for DD Boost provides details.

3. If you plan to migrate existing save sets to the new DD Boost devices, migrate the save sets before the scheduled redirected backups begin. Migration will "seed" the Data Domain system and help to reduce the bandwidth requirements for future backups. Considerations for migrating legacy save sets provides details.
4. Use the NMC Device Configuration wizard to perform the following tasks:
    a. Select or create DD Boost devices on the Data Domain system.

    b. Select or create a Pool resource that is configured to send the save sets to DD Boost devices.

    > ⓘ **Note:** The wizard creates and configures a pool for the Data Domain system that uses only DD Boost devices.

    c. Select or create a NetWorker storage node on which to label and mount the new devices.

    d. Complete the wizard pages.

    Configuring DD Boost devices with the NMC Device Configuration wizard on page 59 provides details.
5. Test the backup environment to ensure that the new configuration operates correctly and that existing backups, that will not use DD Boost devices, continue to run as expected. For backups to new devices, test a restore from those devices.
6. Start the redirection with a full backup to the new devices. This practice avoids a dependency on the last full backup that is stored with the legacy storage environment and the potential need to restore from two different environments.
7. Monitor backup performance, and adjust the backup schedule to optimize the configuration for maximum throughput or additional clients. Monitoring Data Domain events, statistics, and logs on page 166 provides details.

Migrating data into Data Domain systems

When you successfully redirect client backups to the DD Boost devices, the existing save sets that are stored on the legacy devices or file systems become redundant. You can retain the legacy stored data until the data expires, or you can migrate the legacy data to the new devices.

The decision to retain or migrate the legacy data depends on the requirements that differ between sites, clients, and backup types. For example, you might want to retain most of the legacy data and migrate only the backups of sensitive and high-priority clients or certain backup types.

To help you decide to either retain or migrate the existing save sets, review the following information:

- Retain the existing save sets on the legacy storage system until they expire:
    - Provides a way to make the transition; no migration is necessary.
    - Requires you to maintain the legacy storage for the life of the legacy data.
    - Requires you to maintain the legacy storage environment, to perform recoveries of data on the legacy devices.
    - Provides features for storage, recovery, and clone operations that differ between the legacy data and the new data.
- Migrate the existing save sets to the new DD Boost devices:
    - Frees storage on the legacy storage system for removal or use by other clients.
    - Allows you to "seed" the new devices with the legacy client data. Seeding ensures that subsequent client backups are deduplicated against the legacy data. This practice reduces the bandwidth and time that is required for the first backup window with the new devices.

- Offers more flexible storage features for storage, recovery, and cloning, for example, multiple concurrent operations.
- Maintains the NetWorker browse and retention policies and ensures that NetWorker manages all save sets.

Migration versus native Data Domain replication

It is recommended that you do not use the native Data Domain replication feature to migrate data from one Data Domain system to another. NetWorker cannot track, manage, or recover legacy save sets that Data Domain replicates.

You can use the Data Domain replication feature to seed a new system to migrate the data. For example, you can perform native Data Domain replication over a local connection to quickly seed a new target Data Domain system, which you can then physically send to a distant location. Although NetWorker cannot immediately manage or restore the seeded data, this practice has advantages. The seeded data reduces the otherwise heavy bandwidth that is required for a data migration by using a NetWorker clone operation, or if you do not perform a migration, for the initial full backups to the target system. This practice can be especially effective if the remote location has limited network bandwidth.

Migration methods

Data migration is a one-time NetWorker clone operation which you can customize to different device types and time periods. You can include all the data in the migration or you can select a limited amount of data from a specific timeframe or a specific backup type (for example, weekly full backups).

The details of the migration procedure depend on the method that you use and the granularity of the data that you want to migrate.

- To perform a NetWorker scheduled clone operation, refer to Migrating legacy save sets to DD Boost devices.
- To run a NetWorker `nsrclone` script from a command line, refer to the *NetWorker Administration Guide* for details.
- To perform a NetWorker staging (data movement) operation to move data from an AFTD, refer to the *NetWorker Administration Guide* for details.

Migrating legacy save sets to DD Boost devices

After you choose a migration scenario, you can migrate the existing save sets to DD Boost devices. Part of this procedure requires that you create a special clone pool and configure a clone task.

Before you begin

Perform migrations before the scheduled NetWorker client backups begin using the new devices. Migration will seed the Data Domain system and help to reduce the bandwidth requirements for future backups.

Procedure

1. Decide which migration scenario you need. Migration scenarios provides details.
2. Plan the migration schedule to ensure that sufficient DD Boost devices and bandwidth are available and to ensure minimal impact to the usual backup window.

   > Note: When you migrate existing deduplicated VTL or CIFS/NFS AFTD save sets, the deduplication software reverts the save sets to their native non-deduplicated format. The storage node then reads and stores the save sets in deduplicated format on the new

DD Boost devices. This reversion process occurs for both Data Domain and non-Data Domain storage.

3. Create a clone pool for the DD Boost devices to be used for the migration:
   - In the **Data Source** field, select groups for the migration.

     Typically, you migrate the same groups that you selected for the redirection of backups. Redirecting backups from other devices to DD Boost on page 182 provides details.
   - In the **Target Devices** field, select the DD Boost devices to store the migrated data.

     Creating pools to target DD Boost devices on page 94 provides details.
4. Configure a clone task with the **Write Clone Data to Pool** field that is selected for the clone pool.

   Road map for configuring a new cloning data protection policy on page 133 provides details about the scheduled clone option.
5. Run the clone action, either according to its schedule or by a manual start.

   To manually start the clone action, right-click the workflow that contains the clone action, and select **Start**.
6. After the clone operation is completed, verify that the cloned data appears on the target devices.

   DD Boost Conversion and Upgrade on page 181 provides details about the verification of NetWorker operations.
7. After you have verified the cloned save sets, remove the original save sets, as required.
8. If you remove the original save sets, remove unused devices and pools, as required. You cannot delete a pool until you delete or relabel in other pools all the volumes that belong to that pool.
9. To ensure that adequate storage capacity is available, monitor the Data Domain system. Monitor a complete backup cycle of all clients, including save set expirations.

   DD Boost Conversion and Upgrade on page 181 provides details.

Migration scenarios

You can migrate existing backup data from legacy devices or file systems to DD Boost devices. The best scenario for your situation depends on the storage environment configuration and the available capacities and bandwidth.

Migration to DD Boost from conventional tape or AFTD

In the following two migration scenarios, you have added a Data Domain system to the existing NetWorker storage environment. You want to migrate and deduplicate the current legacy data, which is stored on tape or conventional disk, to DD Boost devices on the new system. The reason for this migration could be that you want to remove the old tape or disk system, or free up space on the old system for other clients.

The number of client migrations that you will perform depends on whether you want to seed the devices for future backups or migrate all the legacy save sets. Dell EMC recommends that you seed some of the data, because the new Data Domain system contains no data. If you migrate the data for one client to seed the DD Boost devices and some of the same data exists on other clients, then migrating the data for the additional clients has diminishing seed value.

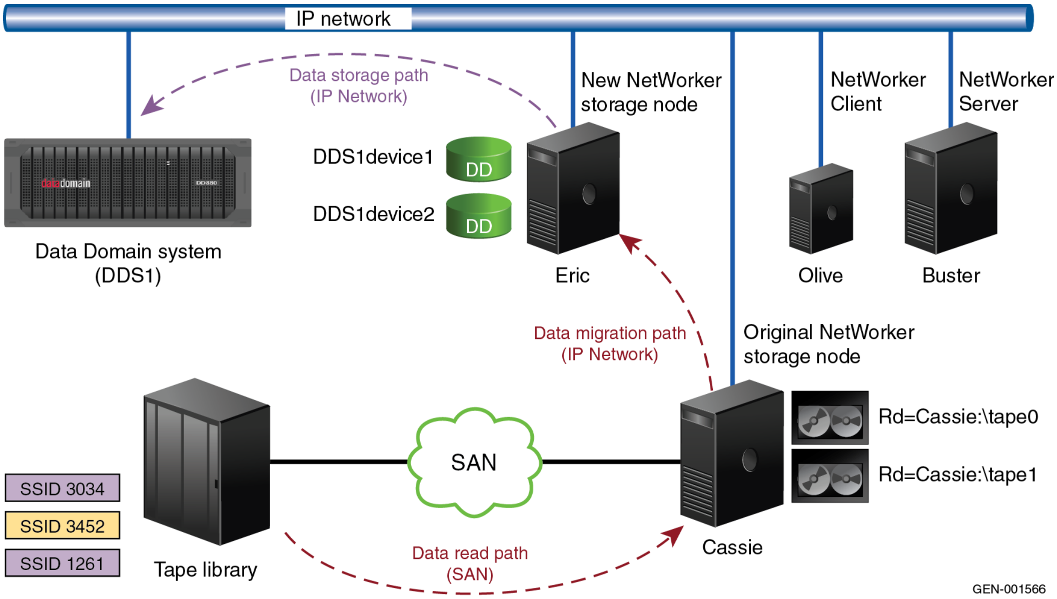
There are two scenarios for this type of migration. In the first case, you create the DD Boost devices on a new storage node. In the second case, you create the devices on the existing storage node.

Migration to new devices on a different storage node

The following figure illustrates a scenario where the storage node named Cassie stored backups of the client that is named Olive on tape or conventional disk. You want to migrate these backups to a different storage node named Eric for storage on the Data Domain system.

In this scenario, you use the IP network to transfer the data from the original storage node Cassie to the new storage node Eric. The time that is required for the transfer depends on the capacity and bandwidth available on the IP network, regardless of the fact that the tape library is on a SAN. If restore operations must use the IP network during the transfer, then additional bandwidth is required to ensure that the data transfer does not impact these operations.

Figure 55 Migration from conventional storage to DD Boost devices on a different storage node



Migration to new devices on the same storage node

You can eliminate data migration over the IP network between storage nodes by migrating data between devices on the same storage node. The following figure illustrates a scenario where you migrate data to DD Boost devices that were created on the original storage node named Cassie. During the migration, the storage node reads the data that is stored on tape or conventional disk and sends the deduplicated data to the Data Domain system for storage.

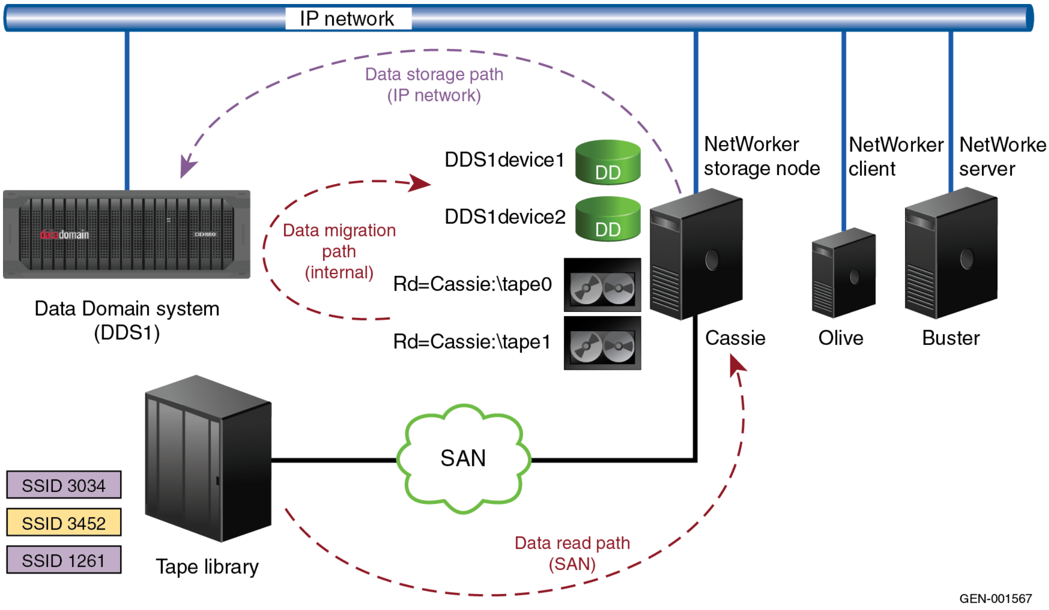
Although this scenario appears to be an ideal solution that avoids IP network restrictions, consider the following factors:

- The existing storage node might be older and already at or near capacity. This situation limits the number of devices that you can add and the amount of data that you can transfer during backup operations.
- The existing storage node might not have extra network connections available. If you need the legacy connections for backup and restore operations, this situation leaves limited bandwidth available for the additional DD Boost format.
- The network connection might not have the recommended 10 GB capacity to maximize throughput from the storage node to the DD Boost devices.

- Although you use the same storage node for the same backup clients, you must change the device allocations and the pools. These changes can add confusion and result in configuration errors.

There are also advantages to this scenario. For smaller sites, to avoid network restrictions you can migrate the data to new devices on the same storage node. This scenario could also be an option for larger sites where you want to reuse multiple storage nodes or reconfigure the storage nodes to share one or more Data Domain systems. You can configure a storage node for data migration to seed the DD Boost devices as an interim step.

Figure 56 Migration from conventional storage to DD Boost devices on the same storage node



Migration to DD Boost from deduplicated VTL or AFTD storage

In the following two migration scenarios, you are already using an existing Data Domain system for VTL or CIFS/NFS AFTD deduplication storage. You want to migrate the stored data to new DD Boost devices on this same Data Domain system. Because the data is already present on the Data Domain system, you do not need to migrate the data to seed the DD Boost devices. The global deduplication format ensures that NetWorker does not resend data that exists on the Data Domain system.

These migration scenarios offer multiple concurrent operations for storage and recovery and more flexible storage options for cloning.

Although these migration scenarios use the same Data Domain system, you must change the pools and the device allocations to redirect the backups to the DD Boost devices. Copy or clone the save sets to migrate the data.

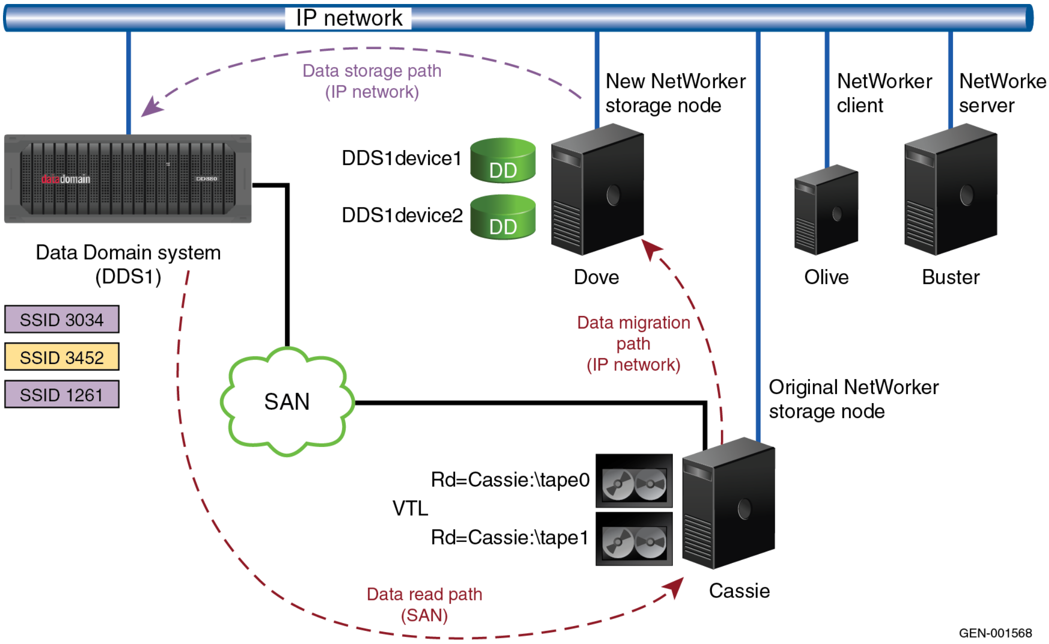
When you migrate existing deduplicated VTL or CIFS/NFS AFTD save sets, the process initially reverts the save sets to their native non-deduplicated format. The storage node then reads and concurrently stores the save sets in a deduplicated format on the new DD Boost devices. Data that exists in a deduplicated format on the Data Domain system is not deduplicated again. During the migration, only the metadata for the save sets are unique.

Migration to new devices on a different storage node

The following figure illustrates a legacy scenario where the storage node Cassie, stored backup data from the client that is named Olive in VTL format over a SAN connection. You want to migrate this data to the new DD Boost devices on a different storage node named Dove.

This migration uses the SAN and the IP networks in two separate stages. First, the original storage node Cassie reads the non-deduplicated data that is provided by the Data Domain system over the SAN connection. Then the new storage node Dove reads this data and concurrently stores only unique data, in this case only the storage metadata, across the IP network to the Data Domain system. The limiting factor is the speed of the transfer across the IP network.

Figure 57 Migration from VTL to DD Boost devices on a different storage node

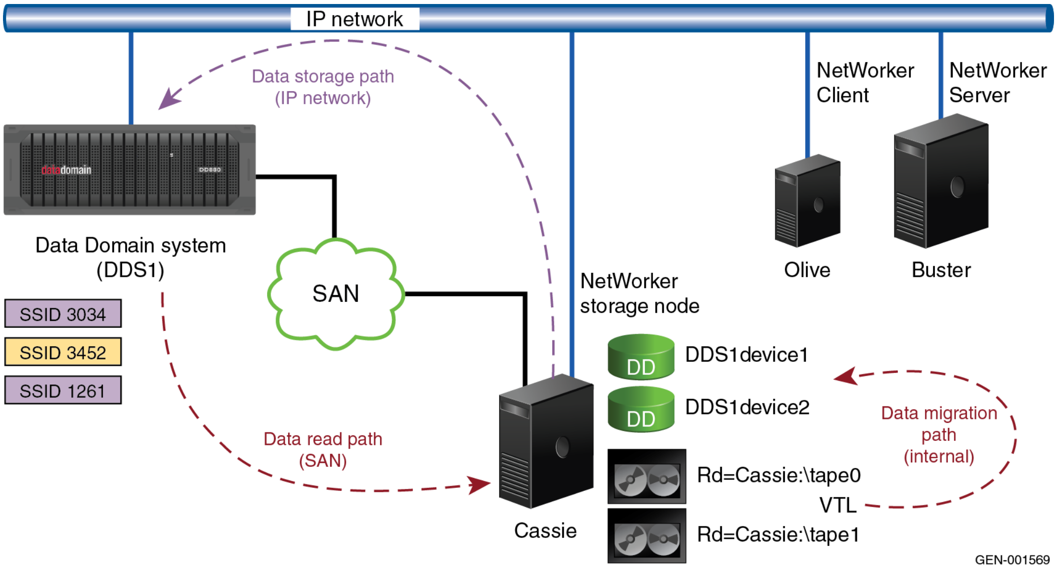


Migration to new devices on the same storage node

The following figure illustrates a scenario where you want to migrate legacy backup data from the client that is named Olive to new DD Boost devices on the original storage node named Cassie. The existing storage node configuration is for VTL storage on a SAN. You have added the configuration for the new DD Boost devices that use the IP network.

Because this migration is between devices on the same storage node, this scenario fully uses the speed of the existing SAN connection. The storage node Cassie reads non-deduplicated data over the SAN and concurrently stores only unique data, in this case only the storage metadata, across the IP network to the Data Domain system.

Figure 58 Migration from VTL to DD Boost devices on the same storage node



GLOSSARY

This glossary contains definitions for terms used in this guide.

A

administrator Person who normally installs, configures, and maintains software on network computers, and who adds users and defines user privileges.

advanced file type device (AFTD) Disk storage device that uses a volume manager to enable multiple concurrent backup and recovery operations and dynamically extend available disk space.

attribute Name or value property of a resource.

authorization code Unique code that in combination with an associated enabler code unlocks the software for permanent use on a specific host computer. **See** license key.

B

backup

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

bootstrap Save set that is essential for disaster recovery procedures. The bootstrap consists of three components that reside on the NetWorker server: the media database, the resource database, and a server index.

C

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

Client Direct Feature that enables clients to deduplicate backup data and send it directly to AFTD or DD Boost storage devices, bypassing the NetWorker storage node. The storage node manages the backup devices but does not handle the backup data.

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

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

clone

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

clone-controlled replication (CCR)

Creation of a replica of deduplicated data copied from one DD Boost device to another, which can be scheduled by the NMC clone feature and is indexed and tracked by the NetWorker server.

D

database

1. Collection of data arranged for ease and speed of update, search, and retrieval by computer software.
2. Instance of a database management system (DBMS), which in a simple case might be a single file containing many records, each of which contains the same set of fields.

datazone

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

DD Boost

Optimized library and communication framework with a special Data Domain API that allows the backup software to define and interact with storage devices on the Data Domain system.

DD Boost device

Logical storage device created on a Data Domain system that is used to store deduplicated NetWorker backups. Each device appears as a folder on the Data Domain system and is listed with a storage volume name in NMC.

DD OS

Data Domain operating system.

deduplication

Process used to compress redundant data.

deduplication backup

Type of backup in which redundant data blocks are identified and only unique blocks of data are stored. When the deduplicated data is restored, the data is returned to its original native format.

deduplication ratio

Reduction in storage space required to store data as a result of deduplication technology, usually combined with data compression, for example, a 20:1 space reduction.

device

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

disaster recovery

Restore and recovery of data and business operations in the event of hardware failure or software corruption.

distributed segment processing (DSP)

Part of the DD Boost interface, which enables data deduplication to be performed on a host before the data is sent to the Data Domain system for storage.

E

enabler code Unique code that activates the software:

- Evaluation enablers or temporary enablers expire after a fixed period of time.
- Base enablers unlock the basic features for software.
- Add-on enablers unlock additional features or products, for example, library support.

See license key.

G

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

H

host Computer on a network.

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

I

ifgroup A private network configured on the Data Domain system consisting of multiple network interfaces logically designated as a single group IP address. The ifgroup provides dynamic load balancing, fault tolerance within the group, and better network bandwidth usage than traditional network aggregation.

L

label Electronic header on a volume used for identification by a backup application.

license key Combination of an enabler code and authorization code for a specific product release to permanently enable its use. Also called an activation key.

M

managed application Program that can be monitored or administered, or both from the Console server.

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

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

metadata Hash information that identifies stored sub-file information for deduplication, and is required to revert deduplicated client backup data to the regular nondeduplicated format.

MTree Shortened from "managed tree," also referred to as storage units, logical partition of the namespace in a Data Domain file system that can be used to group a set of files for management purposes. MTrees are normally associated with a single NetWorker datazone.

N

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

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

notification Message sent to the NetWorker administrator about important NetWorker events.

O

online indexes Databases located on the NetWorker server that contain all the information pertaining to the client backups (client file index) and backup volumes (media index).

optimized clone See clone-controlled replication (CCR)

P

pathname Set of instructions to the operating system for accessing a file:

- An absolute pathname indicates how to find a file by starting from the root directory and working down the directory tree.
- A relative pathname indicates how to find a file by starting from the current location.

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

pool

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

R

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

remote device

1. Storage device that is attached to a storage node that is separate from the NetWorker server.
2. Storage device at an offsite location that stores a copy of data from a primary storage device for disaster recovery.

replication Process of creating an exact copy of an object or data. This is different than NetWorker cloning. **See** clone

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

resource database NetWorker database of information about each configured resource.

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

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

retrieve To locate and recover archived files and directories.

S

save NetWorker command that backs up client files to backup media volumes and makes data entries in the online index.

save set

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

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

save stream Data and save set information that is written to a storage volume during a backup. A save stream originates from a single save set.

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

storage device **See** device.

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

storage unit (SU) Logical unit of disk storage on a Data Domain system that is associated with a NetWorker datazone.

T

trap Setting in an SNMP event management system to report errors or status messages.

V

virtual tape library (VTL) Software emulation of a physical tape library storage system.

volume

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

volume name Name that you assign to a backup volume when it is labeled.