EMC Data Domain and Veritas NetBackup 8.0 and Later Integration Guide

March 2018

A Dell EMC Data Domain Integration Guide

Revisions

Date	Description
March 2018	New IG release for NBU 8.x

Table of contents

PREFACE

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

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

Note

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

Purpose

This document provides information needed to integrate an EMC Data Domain system as a backup target for the Veritas NetBackup (NBU) 7.0 and later storage software from Symantec-Veritas.

Related documentation

To view and download Veritas NetBackup documentation, visit https://www.veritas.com/support/en_US/article.000116412

Special notice conventions used in this document

EMC uses the following conventions for special notices:

DANGER

Indicates a hazardous situation which, if not avoided, will result in death or serious injury.

WARNING

Indicates a hazardous situation which, if not avoided, could result in death or serious injury.

CAUTION

Indicates a hazardous situation which, if not avoided, could result in minor or moderate injury.

NOTICE

Addresses practices not related to personal injury.

Note

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

Typographical conventions

EMC uses the following type style conventions in this document:

Bold	Use for names of interface elements, such as names of windows, dialog boxes, buttons, fields, tab names, key names, and menu paths (what the user specifically selects or clicks)
Italic	Use for full titles of publications referenced in text
`Monospace`	Use for: System code System output, such as an error message or script Pathnames, filenames, prompts, and syntax Commands and options
`Monospace italic`	Use for variables
`Monospace bold`	Use for user input
[ ]	Square brackets enclose optional values
|	Vertical bar indicates alternate selections - the bar means "or"
{ }	Braces enclose content that the user must specify, such as x or y or z
...	Ellipses indicate nonessential information omitted from the example

Where to get help

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

Product information

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

Technical support

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

Your comments

Your suggestions will help us continue to improve the accuracy, organization, and overall quality of the user publications. Send your opinions of this document to BRSdocumentation@emc.com.

Product Introduction

Veritas NetBackup software from Veritas is a heterogeneous backup and recovery suite for large-scale enterprises. NetBackup provides backup, recovery, archive, retrieval, and disaster recovery with pools of storage units.

The three main types of NetBackup software installation options are described in the following table.

NetBackup Software Installation Types

Software Type	Description
Master Server	Installed on a master server machine. Manages device selection, media, backups, archives, and restores.
Media Server	Installed either on the master server machine or on one or more separate media server machines. Provisions the storage devices and manages the backup target such as a disk storage unit or virtual tape drive. (Also called a device host, a storage server, or a data mover.)
Client	Installed on a client machine to be backed up. Sends backup data and receives data on restore operations.

A server may have all three types of software: master, media, and client. In that case, the server can back itself up to a locally-connected disk or tape.

Product Installation

For information about installing the NetBackup software, refer to the *Veritas NetBackup Installation Guide*.

Note

When this document refers to any UNIX or UNIX-based operating system such as Linux, HP-UX, or Solaris, the term UNIX operating system is used.

Terms

The following EMC Data Domain and NetBackup-specific terms are used in this document.

Term	Definition
Data Domain system	A standalone Data Domain storage appliance, gateway, or a single controller in a DDX array.
High water mark (HWM)	The specified highest capacity level for a disk Storage Unit. When HWM is reached, the specified action is taken, for example, the NetBackup administrator is notified or staging to tape begins.
Low water mark (LWM)	The specified lowest capacity level for a disk Storage Unit.
NetBackup Job	A backup, restore, duplicate, verify, import, or image-clean operation. Each job is identified by a Job ID.
OpenStorage (OST)	An intelligent disk storage option that is an API level integration with third party disk vendors. Enables disk backups without tape emulation. The OST Storage Unit type configuration is highly recommended over the Basic Disk Storage Unit type. The main reasons are ease of use and the fact that the OST Storage Lifecycle Policy (SLP) integrates OST Storage Units efficiently into NetBackup's storage plan and data management. In addition, configuration of backups to OST Storage Units with SLP allows optimized duplication. See the *Veritas NetBackup Administrator's Guide* for detailed information about SLP. For configuration instructions, see the *Data Domain Boost for OpenStorage Administration Guide*.
Policy	The information that defines backups; includes clients to be backed up, the storage type to use, the NetBackup media server to use, backup

Term	Definition
	schedules, data types, and data classes. Also called backup policy.
Storage Lifecycle Policy (SLP)	A backup plan that specifies which backup data is copied, which storage units are used, and how long data is stored. All Storage Unit types except Basic Disk can be configured in an SLP. SLPs may be reused by multiple backup policies, so a change to an SLP is easily propagated.
Storage Unit	The device where backup data is stored. The smallest unit of NetBackup storage. The Data Domain system supports the following types of Storage Units: Disk Storage Units, of which there are two types: Basic Disk, which uses an NFS file system or CIFS share on the Data Domain system OpenStorage, which employs a special plugin on the backup server. A DD Boost license is required on the Data Domain system. Only NFS- or CIFS-mounted Basic Disk Storage Units are supported. Network Data Management Protocol (NDMP) Storage Units, which support backups from NDMP-enabled Network Attached Storage (NAS) filers to a Data Domain system that is configured as a virtual tape library (VTL). Media Manager Storage Units, where the Data Domain system is a VTL that emulates a physical tape library and is connected directly to the backup server.

Differences Between File Device and VTL Storage Units

NetBackup can use a Data Domain system as a file device if the Data Domain System is configured with either the Basic Disk (NFS, CIFS) or OST Storage Unit configuration.

The differences between use of the Data Domain system as a file device or as a VTL Storage Unit are as follows:

A Disk Storage Unit (either Basic Disk or OpenStorage) can take advantage of the random-access nature of disks.

When a Data Domain system is used as a VTL (as a NetBackup Media Manager or NDMP Storage Unit), the system emulates a physical tape library and physical tape drives. It retains the characteristics of real tape, but there are no mechanical delays for tape library media motion commands or tape drive positioning commands.

Media Manager or NDMP Storage Unit (VTL)	Disk Storage Unit
A changer driver and tape driver that have been tested and posted as supported in the Data Domain compatibility matrix must be installed and loaded on the NetBackup media server.	No changer driver and tape driver installation and loading is required on the NetBackup media server. If you are using OpenStorage, you must install the appropriate plugin.

A Fibre Channel HBA that has been tested and posted as supported in the Data Domain compatibility matrix must be installed on the NetBackup media server.	A Fibre Channel HBA is not required, unless you are using DD Boost over Fibre Channel with OpenStorage.
Because a VTL emulates a PTL, the backup software has to perform tape mounts, loads, labeling and other tape-emulation tasks even though there are no tapes.	No tape mounts, loads, labeling or other tape emulation tasks are performed.
Expired backup images are not cleaned up on the Data Domain system. Pro—NetBackup can execute its tape import procedure to quickly recover and restore backup images. Con—Expired disk space cannot be recycled immediately when garbage collection and cleaning kicks off.	Expired backup images are cleaned up on the Data Domain system. Pro—Expired disk space is recycled immediately when garbage collection and cleaning kicks off. Con—NetBackup is not able to recover and restore backup images as quickly.
Replication is easier. There is no need to configure CIFS access or NFS access to the Storage Unit.	CIFS or NFS mounts of the Data Domain system must be configured with the proper mount options on the NetBackup media server.
If data needs to be restored from a tape that is in use for a backup, the backup must be stopped in order to proceed with the restore because tape drives are sequential access devices.	Data can be restored from a disk storage unit while a backup is in process to the same storage unit.

Restrictions and Limitations

This section describes restrictions and limitations when they affect NetBackup integration with Data Domain systems.

VTL Restrictions

When the Data Domain system is configured as a Basic Disk Storage Unit, the following actions are likely to mark media changers and tape drives as `DOWN` because NetBackup polls devices periodically and will find that VTL tape drives are inaccessible:

- Data Domain system reboot
- Data Domain VTL restart
- Data Domain file system restart
- Scsitarget disable and re-enable
- Data Domain VTL port disable and re-enable

To detect the possible removal of any devices, perform the following procedure after any of the above actions.

Verify Discovery of Media Changers and Tape Devices

Procedure

1. For Windows, go to **Start** > **Settings** > **Control Panel** > **Administrative Tools** > **Computer Management** > **Device Manager**. Verify that the media changers and tape devices are discovered. For other operating systems, use the appropriate command.
    - `ioscan` on HP-UX
    - `fcinfo` on Solaris
    - `lsscsi` on Linux
2. If the devices are not present, perform the appropriate actions on the physical level and the operating system level and perform Step 1 again.

    For example, verify that the Data Domain system has rebooted properly, or rescan in Windows Device Manager. For other operating systems, use the appropriate command to rescan:
    - `ioscan` on HP-UX
    - `cfgadm` on Solaris
    - `rescan-scsi-bus.sh` on Linux
3. Once the devices are discovered by the operating system, use the NetBackup Administration Console to **UP** the drives in Device Monitor.

After you finish

Some operating systems may renumber tape device special files (that is, assign different file names) while rescanning. This is not a Data Domain system issue. This issue is related to the order in which the operating system scans its SCSI and Fibre Channel buses. If device renumbering occurs, you may need to reboot the NetBackup media server.

One way to avoid device renumbering is to use persistently-named devices. NetBackup can use persistently-named devices on HP-UX 11iv3, but not on Linux.

For more information, see *Integrating the Data Domain System VTL with a Storage Area Network (for Open Systems)*.

Filesystem Restrictions

When the Data Domain system is configured as a file device using NFS, always use either the **`nolock`** or **`llock`** mount option (depending on the operating system version). These options are required because by default NetBackup media servers try to lock the files but fail; locking of files via NFS is not supported on a Data Domain system.

Note

Refer to the *EMC Data Domain Operating System Initial Configuration Guide* and to the documentation for the NetBackup media server's operating system for other recommended mount options.

Microsoft Cluster with Data Domain VTL Restrictions

The following restrictions apply when a Data Domain system is configured as a VTL Storage Unit with Microsoft Cluster nodes:

Both Microsoft Cluster nodes (initiators) connected to the Data Domain VTL must have HBAs from the same HBA vendor. This avoids issues with device port mapping of the changer that occur if different HBA vendors are used in the cluster nodes.

Both cluster nodes must run version 4.4.2.x.x or a higher release.

The IBM LTO driver must be at version 6.1.8.0 or higher for use with the 64-bit version of Windows. For information about installing drivers, refer to the *IBM Tape Drivers Installation and User's Guide* at: www.ibm.com/support/fixcentral. You can also download the driver from that location.

Software Configuration

You can use the wizards in the NetBackup Administration Console to configure storage and policies. The next figure shows the NetBackup Administration Console with the configuration wizards in the right pane.

Note

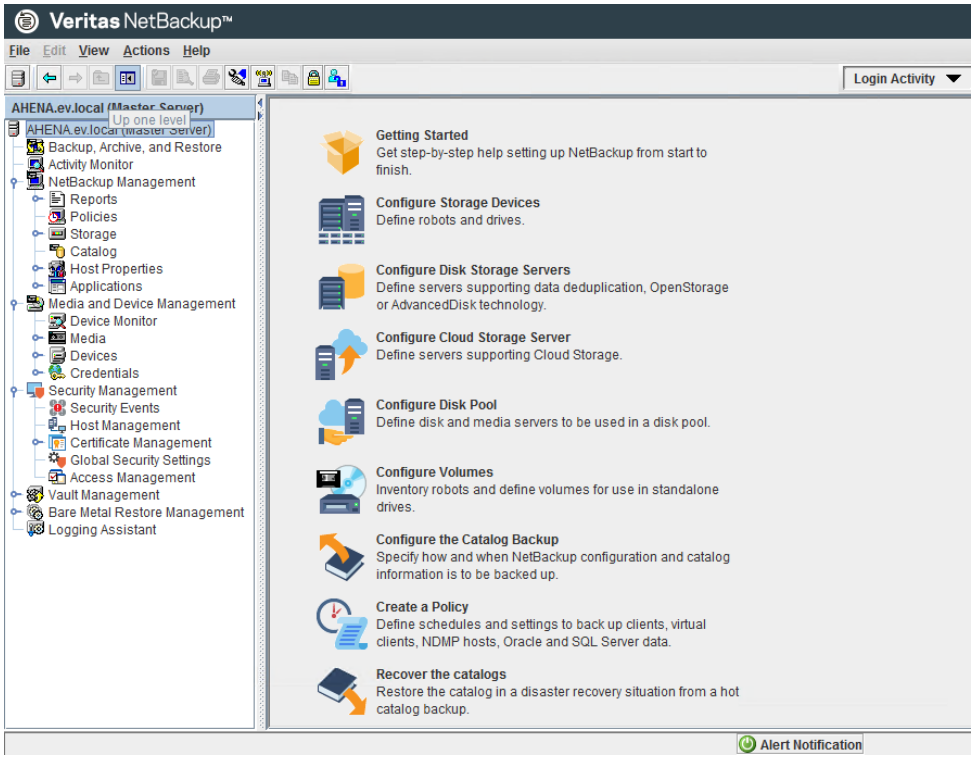
All NetBackup Administration Console examples are from NetBackup.

Note

In command examples when you can enter a path in either a UNIX or Windows operating system, -> is shown as a path separator, instead of either (\) or (/). For example, if an example shows `install->bin`, you would type `install/bin` (UNIX) or `install\bin` (Windows).

Note

In this document, the NetBackup Administration Console is referred to as the NetBackup console.



NetBackup Console

Open the NetBackup Console

The two following procedures describe how to open the NetBackup console.

Open the NetBackup Console on a UNIX Operating System

Procedure

Log in as a user authorized to run NetBackup to an NetBackup master or media server that runs a UNIX operating system.

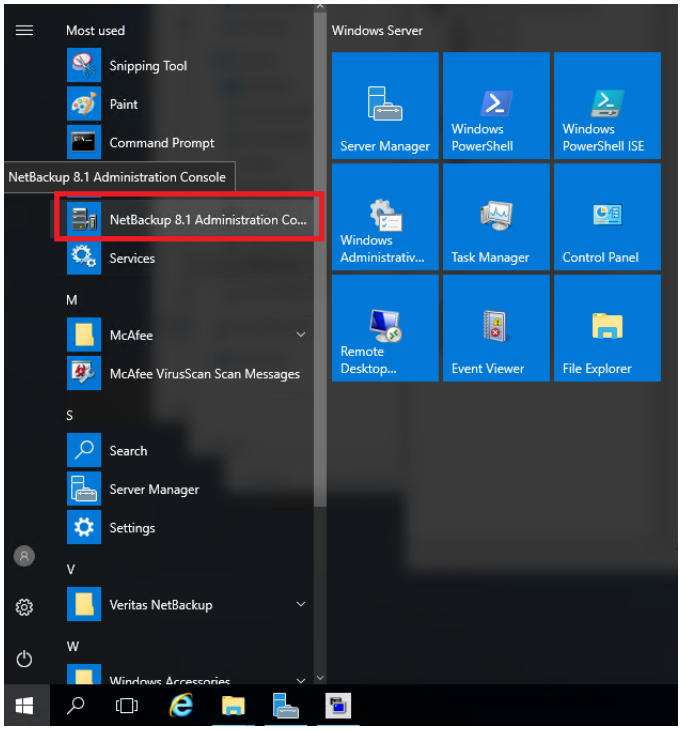
Enter `/opt/openv/netbackup/bin/jnbSA&` on the command line.

Open the NetBackup Console on a Windows Operating System

Procedure

Log into the Windows server as a user authorized to run NetBackup.

Select **Start** > **All Programs** > **Veritas NetBackup** > **NetBackup Administration Console**.



Open an NetBackup Console on a Windows Operating System

View Licenses

On the Data Domain system and on NetBackup, advanced features and most add-ons require additional licenses. For example, NetBackup's Shared Storage Option (SSO) is a licensed feature, and replication is a licensed feature in the Data Domain system.

The two following procedures describe how to view the needed licenses.

View Data Domain System Installed Licenses

Procedure

1. Connect to a Data Domain System Manager Web console.
2. Select **Licenses.**

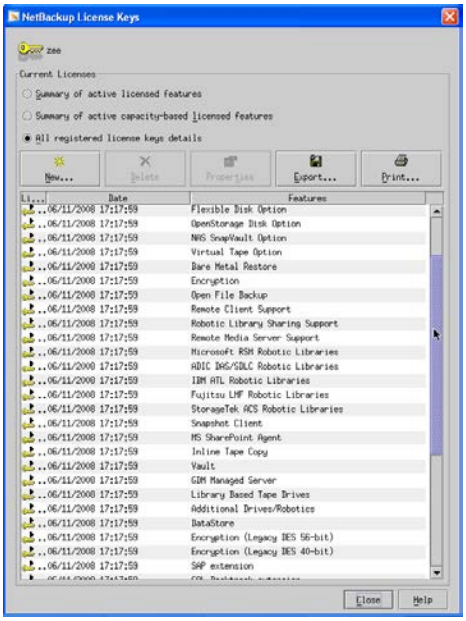
Review NetBackup Installed Licenses

Procedure

Run `get_license_key` from the *`NetBackup_install_path`*`->netbackup->bin->admincmd` directory.

Click **Help** on the NetBackup Administration Console and select **License Keys** to view the installed licenses.

The next figure shows an example of installed licenses displayed on a Windows server.



Installed NetBackup Licenses on a Windows Server

BasicDisk Storage Unit Configuration

A Data Domain system can be configured as a BasicDisk Storage Unit when it is either NFS—or CIFS—mounted on a NetBackup media server.

On a NetBackup media server that runs a version of the Windows operating system, you can specify the absolute pathname to directory to access the Data Domain system with either the Universal Naming Convention (UNC) or the DFS path name.

NFS Guidelines

The example shows a NFS mount of a Data Domain system volume on a non-production UNIX system. Refer to the *EMC Data Domain Operating System Initial Configuration Guide* for recommended mount options.

NFS-mounted Volume on a Non-production UNIX System

CIFS Guidelines in a Windows AD Environment

In an Active Directory (AD) environment, the NetBackup server may fail to connect to a Data Domain system with the default system account if DNS and AD parameters are not set up correctly. Make sure all the needed set up is performed, as described in Configure DNS and AD Entries for the Data Domain System.

Also in an AD environment, Distributed File System (DFS) pathnames provide more-convenient access to Data Domain system targets for disaster recovery. When you configure a CIFS Basic Disk

Storage Unit on a NetBackup media server in a Windows AD environment, use the DFS path name to specify the path to a Data Domain system as described in CIFS Guidelines in a Windows AD Environment.

Configure DNS and AD Entries for the Data Domain System

Procedure

1. On the Data Domain system, perform these steps:
    a. Configure the domain name.
    b. Configure the Data Domain system hostname using the fully qualified name.
    c. Configure an entry for the DNS server.
2. On the DNS server, make sure that DNS host entries are set up for the Data Domain system for both forward and reverse lookups.
3. Verify that an entry for the Data Domain system exists with the correct fully qualified name in the AD tree.

Configure DFS Shares on a Windows NetBackup Media Server

About this task

Perform the following configuration steps to set up a Data Domain system with DFS shares on a NetBackup media server that runs Windows.

Procedure

1. Create an active/passive setup for the distributed filesystem target for DR, restore or vaulting from the secondary Data Domain system. Make sure the secondary Data Domain system does not have a mapped DFS share that is active.
2. When the secondary Data Domain system is ready to be used for disaster recovery (DR), restore or vaulting activities, reboot the Windows system to clear the Windows cache.

Data Domain cloud tier

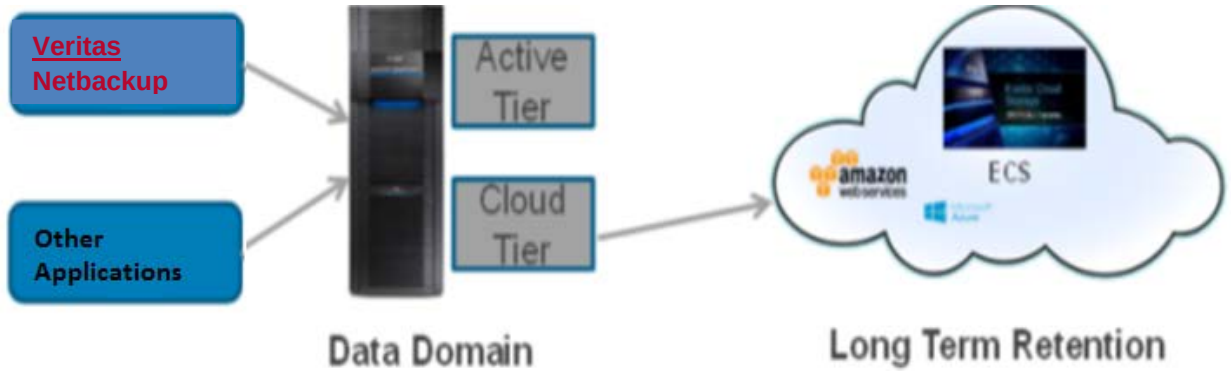
DD Cloud Tier is a Data Domain System feature for moving data from the active tier to low-cost, high-capacity object storage in the public, private, or hybrid cloud for long-term retention. DD Cloud Tier is best suited for long-term storage of infrequently accessed data that is being held for compliance, regulatory, and governance reasons. The ideal data for DD Cloud Tier is data that is past its normal recovery window.

Configure cloud tier as described in the Data Domain Operating System Administration Guide

Configuring Netbackup for Cloud Tier devices

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.

NetBackup allows users to move their backup datasets to data domain active tier location (i.e. mtree) and from there, files are moved to cloud using DDR "data-movement" commands.



Overview of the DD Cloud Tier solution.

To know about Cloud Tier Requirements, Configuring DD Cloud Tier Devices and Cloud data movement schedules, refer to "Data Domain OS 6.1 Administration Guide".

For supported cloud platforms, refer to "Data Domain Cloud Tier Compatibility Matrix".

Important: The example dealt in this Cloud Tier section considered CIFS Protocol i.e. Files are moved from CIFS Share on Data Domain (Mtree) and from CIFS Share files are moved to Cloud Unit. The same procedure is applicable for NFS as well. VTL is not considered.

Perform a test backup - Backing up files to DDR

Here, ECS Cloud is considered as example.

On DDR,
a. Create an ECS Cloud Profile. Here "**ECS**" is the profile name.

```
sysadmin@dd7200-15# cloud profile show

Profile name: ECS
        Provider: ecs
        Endpoint: http://load-vm1.chaos.local:9020
        Proxy host:
        Proxy port: 0
        Proxy username:
sysadmin@dd7200-15#
```

Cloud Profile

b. Create a Cloud Unit. Here "**ecs-unit1**" is the cloud unit name.

```
sysadmin@dd7200-15# cloud unit list
Name         Profile   Status
---------    -------   ------
ecs-unit1    ECS       Active
---------    -------   ------
sysadmin@dd7200-15#
```

Cloud Unit

c. Create "mtree" and create a CIFS share (for windows) using DDSM Console or DDCLI.

Data Management **MTree**

MTree — More Tasks | ?

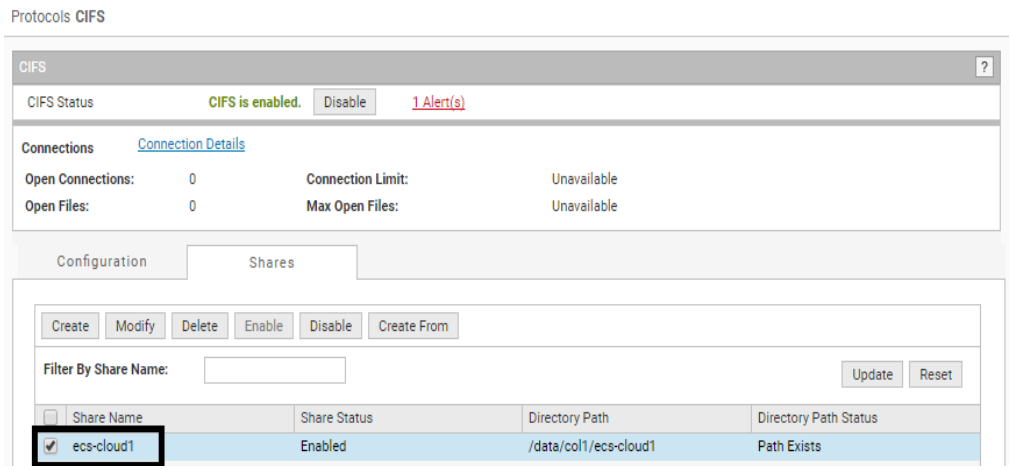
Create | Delete | Manage Schedules

Filter by MTree Name: | Update | Reset

MTree Name	Quota Hard Limit	Last 24hr Pre-Comp	Last 24hr Post-Comp	Last 24hr Comp Ratio	Weekly Avg Post Comp	Last Week Post-Comp	Weekly Avg Comp Ratio	Last Week Comp Ratio
/data/col1/backup	Disabled	0.0 GiB	0.0 GiB	0.0x	0.0 GiB	0.0 GiB(0.0%)	0.0x	0.0x
/data/col1/ecs-cloud1	Disabled	0.0 GiB	0.0 GiB	0.0x	0.0 GiB	0.0 GiB(0.0%)	0.0x	0.0x
/data/col1/nfs	Disabled	0.0 GiB	0.0 GiB	0.0x	0.3 GiB	0.0 GiB(-100.0%)	1.5x	0.0x
/data/col1/new	Disabled	0.0 GiB	0.0 GiB	0.0x	0.5 GiB	0.0 GiB(-100.0%)	25.9x	0.0x

Items Selected: 1 — Items 1-4 of 4

Mtree Creation



CIFS Share Creation

```
sysadmin@dd7200-15# mtree list
Name                          Pre-Comp (GiB)    Status
---------------------------   --------------    ------
/data/col1/backup                        0.0    RW
/data/col1/ecs-cloud1                    0.0    RW
/data/col1/test                          1.6    RW
/data/col1/new                          27.3    RW
---------------------------   --------------    ------
 D     : Deleted
 Q     : Quota Defined
 RO    : Read Only
 RW    : Read Write
 RD    : Replication Destination
 RLGE  : Retention-Lock Governance Enabled
 RLGD  : Retention-Lock Governance Disabled
 RLCE  : Retention-Lock Compliance Enabled
```

List Mtrees

d. Run a file report on this mtree path.

```
sysadmin@dd7200-15# filesys report generate file-location path /data/col1/ecs-cloud1
-------------------------------     ---------------------     ---------------------     --------------------------
File Name                           Location(Unit Name)       Size                      Placement Time
-------------------------------     ---------------------     ---------------------     --------------------------
-------------------------------------------------------------------------------------------------------------------
```

File Report

e. In Netbackup create storage unit as per steps given in section -Configure a BasicDisk Storage Unit
f. Create a backup policy and run the backup job and ensure backup job completes successfully.
g. Now on DDR, again run a file report on this mtree path. Ensure that backup dataset is moved to DDR **Active** tier.

filesys report generate file-location path <mtree_path>

```
sysadmin@dd7200-15# filesys report generate file-location path /data/col1/ecs-cloud1
------------------------------      ---------------------      ---------------------      --------------------------
File Name                           Location(Unit Name)        Size                       Placement Time
------------------------------      ---------------------      ---------------------      --------------------------
/data/col1/ecs-cloud1/36af6e0a05a4e8175009b40000a.fd    Active  1.00 GiB        Thu Jan  4 11:33:40 2018
-------------------------------------------------------------------------------------------------------------------
```

File Report

Perform a test backup - Moving files from Active Tier to Cloud Tier

Ensure data-movement policy is set by running below commands.

data-movement policy show

```
sysadmin@dd7200-15# data-movement policy show
No Mtrees have data-movement policy set.
```

Data Movement - Show

Note: In the below example, default age-threshold of "14" days is maintained.

data-movement policy set age-threshold 14 to-tier cloud clout-tier <cloud_unit_name> mtrees <mtree_path>

```
sysadmin@dd7200-15# data-movement policy set age-threshold 14 to-tier cloud cloud-unit ecs-unit1 mtrees /data/col1/ecs-cloud1
The data-movement age-threshold policy is set to "14" days for the following Mtree(s):
/data/col1/ecs-cloud1
```

Data Movement – Policy Set

```
sysadmin@dd7200-15# data-movement policy show
Mtree                    Target(Tier/Unit Name)    Policy           Value
----------------------   ----------------------    -------------    -------
/data/col1/ecs-cloud1    Cloud/ecs-unit1           age-threshold    14 days
----------------------   ----------------------    -------------    -------
```

Data Movement – Policy Show

Run data-movement command in order to move from Active tire to Cloud tier.

data-movement start mtrees <mtree_path>

```
sysadmin@dd7200-15# data-movement start mtrees /data/col1/ecs-cloud1
Data-movement started.
Run "data-movement watch" to monitor progress.
```

Data Movement - Start

data-movement watch

```
sysadmin@dd7200-15# data-movement watch

Data-movement:
   97% complete; time:  0:03:11
      Moved (post-comp): 166.76 MiB, (pre-comp): 1.00 GiB,
      Files inspected: 1, Files eligible: 1, Files moved: 1, Files failed: 0

Data-movement was started on Jan  4 2018 11:47 and completed on Jan  4 2018 11:51
Moved (post-comp): 166.76 MiB, (pre-comp): 1.00 GiB,
Files inspected: 1, Files eligible: 1, Files moved: 1, Files failed: 0
sysadmin@dd7200-15#
```

Data Movement - Watch

Now, again run file report and ensure file is now available on cloud. Note that the Location of file is now "**ecs-unit1**" instead "**active**".

filesys report generate file-location path <mtree_path>

```
sysadmin@dd7200-15# filesys report generate file-location path /data/col1/ecs-cloud1
------------------------------      ---------------------      ---------------------      --------------------------
File Name                           Location(Unit Name)        Size                       Placement Time
------------------------------      ---------------------      ---------------------      --------------------------
/data/col1/ecs-cloud1/36af6e0a05a4e8175009b40000a.fd    ecs-unit1      1.00 GiB       Thu Jan  4 11:50:10 2018
-------------------------------------------------------------------------------------------------------------------
sysadmin@dd7200-15#
```

File Report

Restore of backed up file

To restore back file(s) from cloud (ECS) to active tier (DDR), file should be recalled and run file report to ensure location is set to "active"

data-movement recall path <file_location>

```
sysadmin@dd7200-15# data-movement recall path /data/col1/ecs-cloud1/36af6e0a05a4e8175009b40000a.fd
Recall initiated for "/data/col1/ecs-cloud1/36af6e0a05a4e8175009b40000a.fd". Run the status command to monitor its progress.
```

Data Movement - Recall

data-movement status

```
sysadmin@dd7200-15# data-movement status
Data-movement to cloud tier:
----------------------------
Data-movement was started on Jan  4 2018 11:47 and completed on Jan  4 2018 11:51
Moved (post-comp): 166.76 MiB, (pre-comp): 1.00 GiB,
Files inspected: 1, Files eligible: 1, Files moved: 1, Files failed: 0

Data-movement recall:
---------------------
No recall operations found.
```

Data Movement - Status

filesys report generate file-location path <mtree_path>

```
sysadmin@dd7200-15# filesys report generate file-location path /data/col1/ecs-cloud1
--------------------------------      ----------------------      ----------------------      --------------------------
File Name                             Location(Unit Name)         Size                        Placement Time
--------------------------------      ----------------------      ----------------------      --------------------------
/data/col1/ecs-cloud1/36af6e0a05a4e8175009b40000a.fd    Active    1.00 GiB        Thu Jan  4 11:59:07 2018
--------------------------------------------------------------------------------------------------------------------------
```

File Report

Now from Netbackup console, run restore job to restore back dataset from DDR to required client file system location.

Configure a BasicDisk Storage Unit

About this task

While logged on to the NetBackup media server as an administrator authorized to run NetBackup, configure the Data Domain system as a BasicDisk Storage Unit with the Getting Started wizard or with menu options on the NetBackup console.

Note

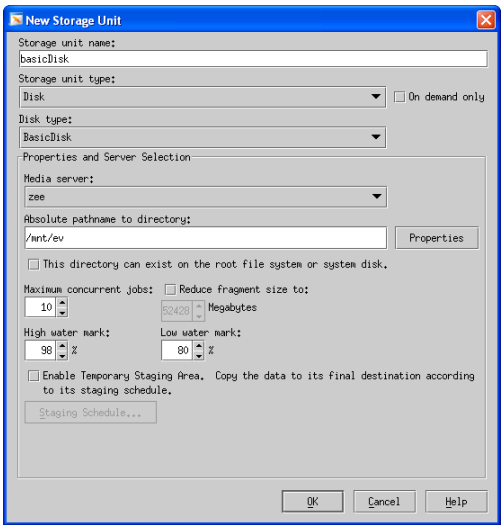
This procedure shows use of menu options on the NetBackup console.

Procedure

1. In the left window of the NetBackup console, select **Storage** > **Storage Units** > **New Storage Unit**.
2. Specify the Storage unit parameters.

   Specify 10 as the maximum number of concurrent jobs (the default value is 1), to allow concurrent jobs to run to this Storage Unit.

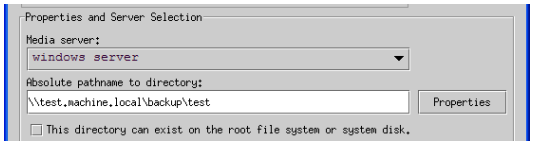
   The next figure shows a successfully configured BasicDisk Storage Unit with a Data Domain system volume on an NetBackup media server that runs a UNIX operating system.



Basic Disk Storage Unit

Note

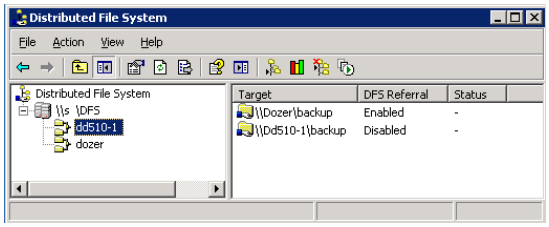
On a NetBackup media server that runs a Windows operating system, you can specify the absolute pathname to directory with either the Universal Naming Convention (UNC) or the DFS pathname to the Data Domain system. The next figure shows an example of a UNC pathname.



Windows NetBackup Media Server With a UNC Pathname

3. To configure a CIFS Basic Disk Storage Unit on a Windows NetBackup media server in an AD environment, enter the DFS path name to the Data Domain system.

   The next figure shows an example of two DFS links on a DFS Server. In this example, the `dd510-1` link contains two targets: `\\Dozer\backup` is enabled while `\\Dd510-1\backup` is disabled.



Example of Two DFS Links

The next figure shows the Absolute pathname to directory that was entered for the DFS link example in the previous figure.

Absolute Pathname to Directory Example

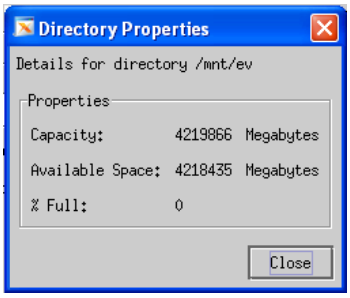
In the example in a non-production configuration, a backup policy uses the DFS basic disk Storage Unit, and the backup destination is the Data Domain system `\backup` directory. Backups are written to `\\Dozer\backup` because `\\Dd510-1\backup` is disabled.

CAUTION

In a production environment, carefully consider the infrastructure requirements so you can create the appropriate BasicDisk directory. It is best practice to create additional backup paths on a Data Domain system under `\backup` for each BasicDisk Storage Unit, for example: `\\Dozer\backup\test`.

A successfully configured BasicDisk Storage Unit also reflects the properties of the Absolute pathname to directory path.

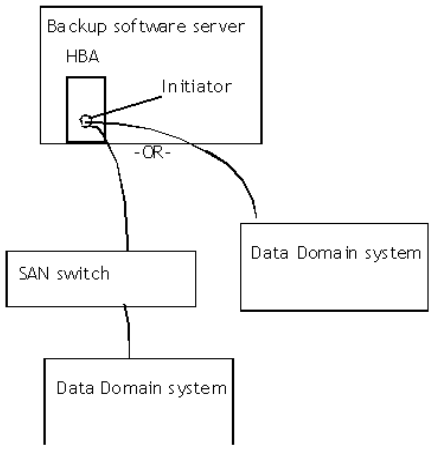
4. Click **Properties** in the Change Storage Unit window. The Directory Properties dialog box appears.



Basic Disk Storage Unit Properties

VTL Storage Unit Configuration

A Data Domain system configured as a VTL Storage Unit is connected to one of the ports on an HBA on the backup software server. The Data Domain system can be connected to the backup software server either directly or through a SAN switch.



Data Domain System Connections for a VTL Configuration

Establish the FC Connection and Install Drivers

Procedure

1. Physically connect and establish a Fibre Channel (FC) connection between the Data Domain system and the NetBackup media server.
2. Make sure the correct changer driver and tape driver are installed and loaded on the NetBackup media server. For the required driver and tape driver refer to the *Backup Compatibility Guide, EMC Data Domain Operating System* for the current DD OS release and the Data Domain system model.
3. Log into the Data Domain system as sysadmin, and enter `vtl initiator show`.

Results

If the Storage Area Network (SAN) connection is set up correctly, the status of the initiator on the NetBackup media server host is shown as Online. The next figure shows initiators that have been configured with aliases on a Data Domain system.

```
sysadmin# vtl initiator show
Initiator      Group               Status   WWNN                      WWPN
Port
------------   -----------------   ------   -----------------------   -------------
----------
----
Broc16GbLin    LinBroc             Online   20:00:8c:7c:ff:3e:6d:01
10:00:8c:7c:ff:3e:6d:01
5a
Brocade16Gb    Direct16GbBrocade   n/a
10:00:8c:7c:ff:3e:6d:00
none
Brocade1860    WindowsBroc         Online   20:00:8c:7c:ff:3d:cc:01
10:00:8c:7c:ff:3d:cc:01
5a
Direct6280B    Direct6280B         Online   20:00:00:24:ff:61:fb:56
```

```
21:00:00:24:ff:61:fb:56
1b
Emulex 16 Gb   Direct16GbEmulex    n/a      n/a
10:00:00:90:fa:10:bc:ec
none
LinEm16Gb      LinEm               Online   20:00:00:90:fa:10:bc:ed
10:00:00:90:fa:10:bc:ed
5a

QlogLin16Gb    LinQlogic           Online   20:00:00:0e:1e:09:d5:b6
21:00:00:0e:1e:09:d5:b6
5a
Qlogic16Gb     Direct16Gb          n/a      n/a
21:00:00:0e:1e:09:d5:b7
none

------------   -----------------   ------   ----------------------   -------------
----------
----
Initiator                 Symbolic Port Name

Address Method
----------------------   ------------------------------------------------------------
----------
------------------------------------------------------------------------------   -----
---------
Broc16GbLin               Brocade-1860-2p | 3.2.3.0 | wknow.backup | Red Hat
Enterprise Linux
Server release 6.4 (Santiago) |  Brocade-1860-2p | 3.2.3.0 | wknow.backup |   auto
Brocade16Gb
                                                                               auto
Brocade1860               Brocade-1860-2p | 3.2.3.0 | WIN-89O53VFHFSD | Windows
Server 2008 R2
Enterprise | Service Pack 1 Brocade-1860-2p | 3.2.3.0 | WIN-89O53VFHFSD |     auto
Direct6280B
                                                                               auto
Emulex 16 Gb
                                                                               auto
LinEm16Gb                 Emulex PPN-10:00:00:90:fa:10:bc:ed Emulex LPe16002-E
FV1.1.43.3
DV8.3.7.18                                                                     auto
QlogLin16Gb               QLE2672 FW:v6.06.03 DVR:v8.05.00.03.06.0-k
                                                                               auto
Qlogic16Gb
                                                                               auto
```

Create a VTL Group on the Data Domain System

Procedure

On the Data Domain system, create a VTL group, and add a VTL and the initiator into the VTL group. Refer to the *EMC Data Domain Operating System Administration Guide* for information about setting up a VTL.

Results

The example shows a valid VTL group with one initiator, one changer, and two drives.

```
sysadmin# vtl group show LinQlogic

Group: LinQlogic

Initiators:
Initiator Alias   Initiator WWPN
---------------   ----------------------
QlogLin16Gb       21:00:00:0e:1e:09:d5:b6
---------------   ----------------------

Devices:
Device Name       LUN   Primary Ports   Secondary Ports   In-use Ports
---------------   ---   -------------   ---------------   ------------
LinQl16 changer     0             all              none            all
LinQl16 drive 1     1             all              none            all
LinQl16 drive 2     2             all              none            all
---------------   ---   -------------   ---------------   ------------
```

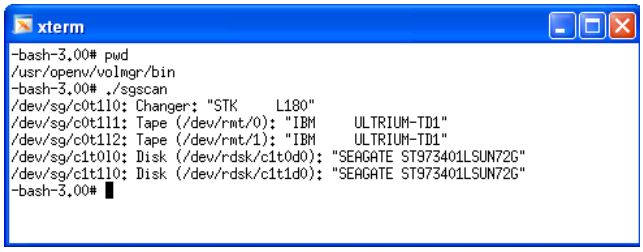
A Valid VTL Group With One Initiator, One Changer, and Two Drives

Configure a VTL on the NetBackup Media Server

Procedure

1. On the NetBackup media server, make sure the devices are discovered. Execute the `sgscan` command in the *`NetBackup_install_path`*`->volmgr->bin` directory.

   The next figure shows the discovered devices when the `sgscan` command is entered on an NetBackup media server that runs a UNIX operating system.



   Output from Command on an NetBackup Media Server

2. If the `sgscan` command does not show any tape devices, perform these additional checks.

   a. At the operating system level, check that the medium changer and tape drives are discovered.

   b. At the HBA level, make sure that the LUNs for both the medium changer and tape drives are discovered.

   c. Make sure that the system kernel has enough targets to accommodate the total number of configured tape drives and changer.

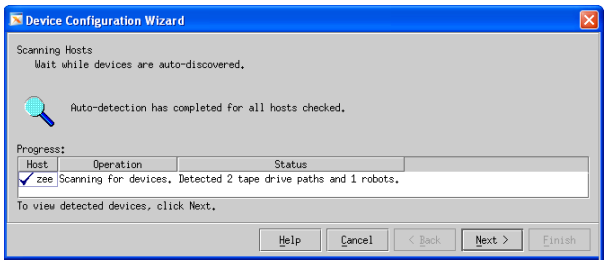
      See the *Veritas NetBackup Device Configuration Guide for UNIX, Windows and Linux* for how to perform the above checks and verifications.

      On Solaris backup servers, follow the instructions in the *NetBackup Device Configuration Guide* (scripts `sg.build` and `sg.install`).

Refer to the *Veritas Netbackup Device Configuration Guide* to complete the device configuration based on the operating system of the NetBackup media server.

3. From the NetBackup console, run the Configure Storage Devices wizard.
4. Select the host that has the Data Domain system VTL attached. Click **Next.**

   NetBackup auto-detection shows the discovered devices. The next figure shows the devices detected on an NetBackup media server.



NetBackup Media Server Auto-detected Tapes and Robot

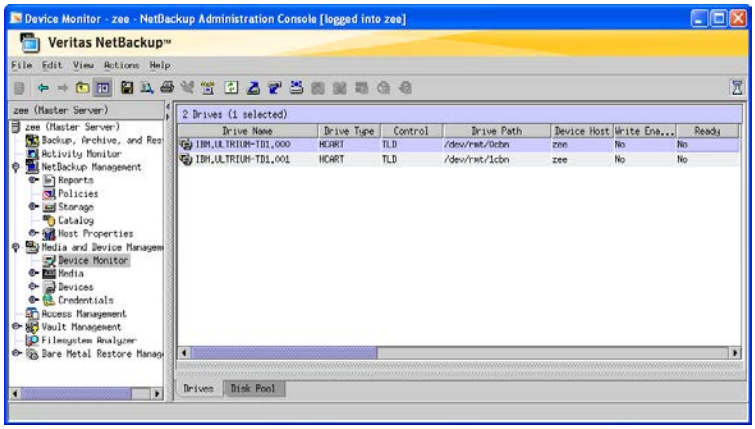
5. Complete the steps in the Device Configuration Wizard.

Verify the VTL Storage Unit Configuration

Procedure

1. Select the **Device Monitor** from the left menu of the NetBackup console.
2. Verify the configuration.

   The Device Monitor shows all configured devices. The next figure shows a successfully configured VTL on an NetBackup media server that runs a UNIX-based operating system.

6. 

   7. Configured VTL Displayed by the Device Monitor

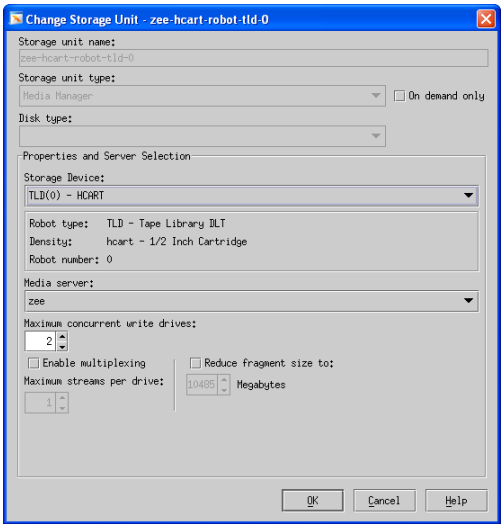
8. Select **Storage** in the right window of the NetBackup console.
9. Right click on the VTL Storage Unit and select **Change**.

Results

The next figure shows the properties of a Data Domain system VTL Storage Unit. The parameters are default values for a VTL that consist of two tape drives.

Note

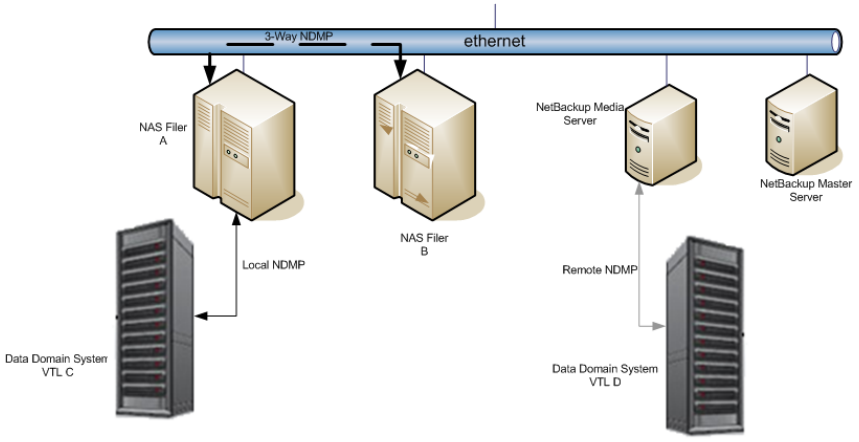
In the next figure, multiplexing is not enabled.



Data Domain VTL Storage Unit

NDMP Storage Unit Configuration

The next figure shows hardware configuration options for NDMP backups: 3-way NDMP, Local NDMP, and Remote NDMP.



NDMP Configuration Options

Type	Definition
Local NDMP	The Data Domain system is logically directly connected to an NDMP NAS filer. In the figure, data from NAS filer A is backed up on the locally attached Data Domain system VTL C.
Remote NDMP	(A NetBackup term) Backups can be made from a NDMP NAS filer to a Data Domain system that is directly attached to a NetBackup media server. In the remote NDMP illustration in the figure, Data Domain system VTL D is attached to an NetBackup media server; data from NAS filer A is backed up to the Data Domain system VTL D. With Remote NDMP, NDMP type backups and non-NDMP type backups can share the same backup devices that are attached to the media server.
3-way	Involves two or more NDMP Data Movers and a Data Mover Agent. For example, in the figure NAS filer B can be backed up to either Data Domain system VTL C or D.

Verify that the NDMP option is installed on the NetBackup media server. For configuration details, refer to the *Veritas NetBackup for NDMP Administrator's Guide for UNIX, Linux, and Windows*.

Verify NDMP Installation on the NetBackup Media Server

Procedure

1. Go to the *`NetBackup_install_path`*`->lib` directory.
2. Verify that the `libndmpclient.so` library file exists in the directory.

Configure an NDMP Storage Unit

Procedure

1. From the NetBackup console, run the Configure Storage Devices wizard.
2. Select the NetBackup media server to configure as the Device Host for NDMP.
3. Click **Change**. The Change Device Host dialog box appears.
4. Perform the following steps.

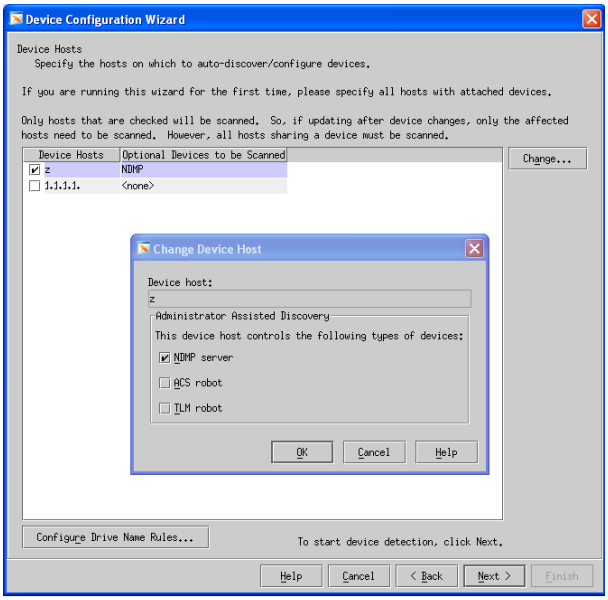
    a. Enter a DNS name in the **Device Host** field. The example shows z as the device hostname.

    b. Click the **NDMP server** checkbox.

    c. Click **OK** to save the configuration and close the dialog box.

    d. Click **Next** in the Device Configuration Wizard.

    The next figure shows an example of a Device Configuration Wizard and the Change Device Host dialog box configured for NDMP set up.



Change Device Host for NDMP Setup

5. Perform the following steps in the NDMP Hosts window.

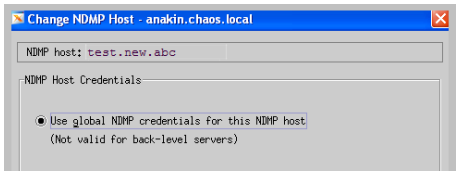
    a. Click **New.**

    b. Add the NDMP host and click **OK**. The New NDMP Host dialog box appears.

6. Configure NDMP credentials.

    Refer to the *NetBackup NDMP Administrator's Guide for UNIX, Linux, and Windows* for details on NDMP Host Credentials. The infrastructure and implementation policy of each site determine the appropriate type of NDMP credentials to configure.

The next figure shows an example of an NDMP host configured to use global NDMP credentials.



NDMP Host test.new.abc With Global NDMP Credential

7. Follow the wizard steps to complete the NDMP configuration.
8. Verify the settings with the `tpautoconf` command with the `–verify –nh` options followed by the name of the NDMP-enabled NAS filer.

   `# tpautoconf –verify –nh ndmp_host_name`

   The following example shows the relevant output of a `tpautoconf verify` command after the host's NDMP credentials are successfully registered and configured.

```
Connecting to host "test.new.abc" as user "root"...
...Host info is:
host name "test.new.abc"
os type "NetApp"
os version "NetApp Release 7.x.x.x"
host id "xxxxx"
Login was successful
Host supports LOCAL backup/restore
Host supports 3-way backup/restore
```

Backup Policy Configuration, Backups and Restores

A backup policy must be configured before backups can be performed.

Note

Because certain required backup policy attributes cannot be configured with the Backup Policy Wizard, the procedure in this section does not use the wizard.

Perform the following tasks to perform backups and restore data on the NetBackup media server.

Configure a Backup Policy

Procedure

1. On the NetBackup console, select **NetBackup Management** > **Policies**.
2. Select **New Policy**. The New Policy dialog box appears.
3. Configure the policy as follows for a backup policy to use for backups to a Data Domain system.
   a. Verify that **Compression** is not selected
   b. Verify that **Encryption** is not selected
   c. Specify **Take checkpoints every: x minutes** when a large volume backup is involved. This allows the backup to restart from the last checkpoint in a case a large volume backup fails for any reason.

d. If a VTL Storage Unit is being used, verify that **Enable multiplexing** is not selected. Disabling multiplexing allows a Data Domain system to compress data efficiently.

Note

The **Limit jobs per policy** setting limits the number of jobs the current backup policy can execute. It limits the number of streams if multiple jobs from the same policy run concurrently, but it does not limit the number of streams per job.

In the Global Attributes that are set from the NetBackup console under Host Properties, the **Maximum jobs per client** setting limits the number of jobs that can be set in any policy.

Manually Run a Back Up

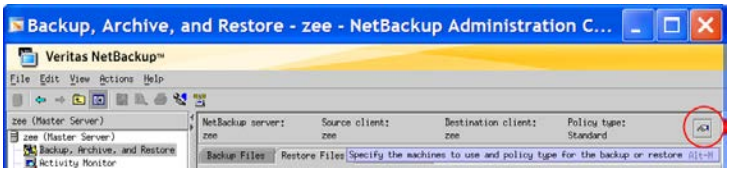
Procedure

1. On the NetBackup console, select the backup policy.
2. Right click on the backup policy and select **Manual Backup**.

Restore Backed Up Data

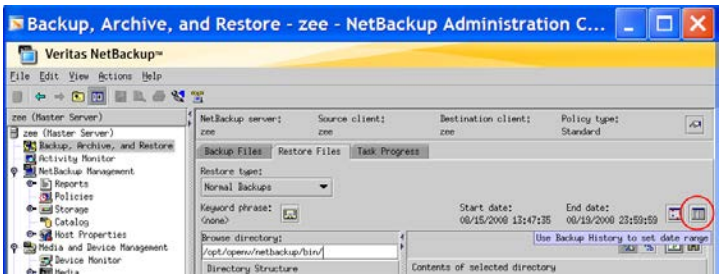
Procedure

1. From the left menu of the NetBackup console, select **Backup, Archive, and Restore**.
2. In the top right of the screen shown in the next figure, select the hand icon to bring up the Specify NetBackup Machines and Policy Type dialog.



Backup Configuration Icon

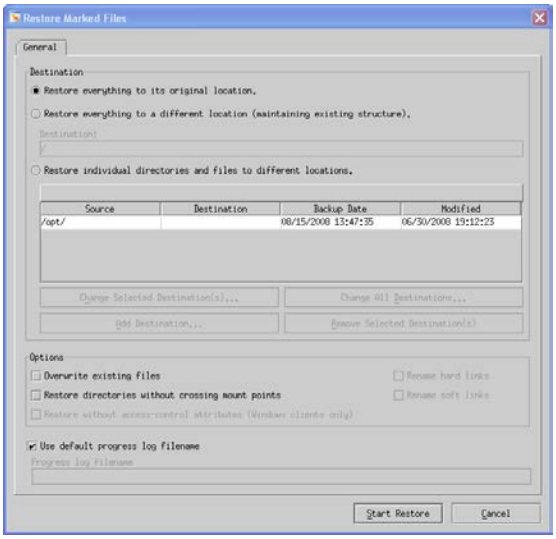
3. After configuring machines and the policy to use in the dialog box, click **OK**.
4. Click the backup history icon to the right of the NetBackup console to bring up the Backup History dialog.



Backup History Icon

5. In the Backup History Dialog, select the backup to be restored and click **OK.**

6. Select the files or directories to be restored and click **Restore**. A Restore Marked Files window appears.
7. Select **Destination and Options**. The next figure shows the selected Destination and Options for a restore example.



Selected Destination and Options for a Restore Example

8. Click **Start Restore** to run the Restore job.
9. Monitor the job from the Activity Monitor.

Configure Required NetBackup Global Settings

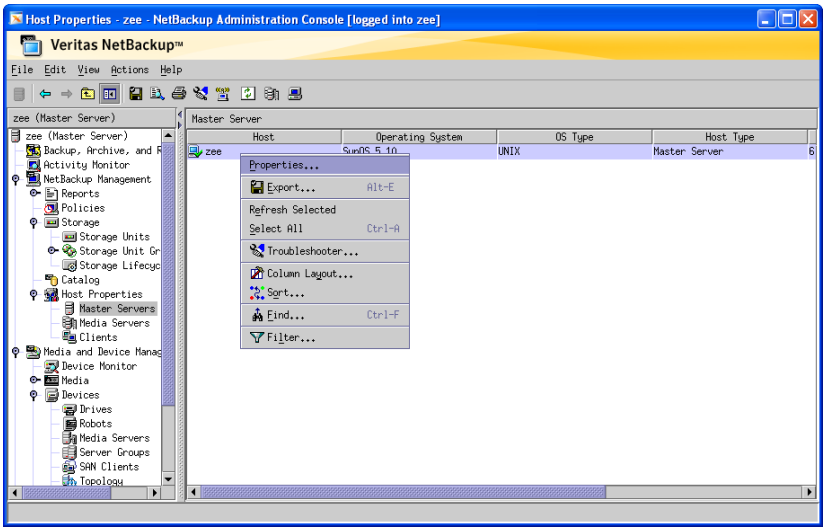
About this task

The NetBackup administrator can choose most parameter settings for the backup policies, Storage Units, the media server, and the master server host properties based on the needs of the site. The following procedures provide the parameter settings that must be used to enable NetBackup to work with a Data Domain system.

Procedure

1. On the left menu of the NetBackup console, select **Host Properties**.
2. Select **Master Servers** and select the host on the right pane of the NetBackup console.
3. Right click and select **Properties.**

   The next figure shows the Properties option selected from the Master Server pull-down menu.



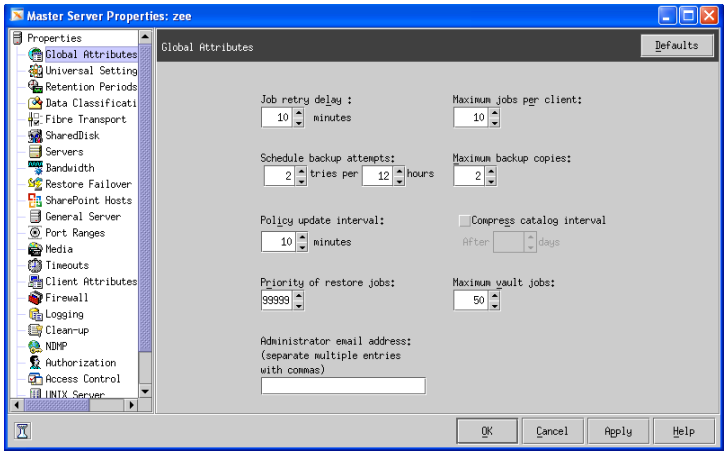
Master Server > **Properties** Option on the NetBackup Console

4. Select **Global Attributes** and set values that apply to all NetBackup media servers.

Note

Global Attributes settings on the master server affect all media servers. Consult with your IT department policy to determine which Global Attributes to implement. The default value of the **Maximum jobs per client** global setting is 1, while Veritas's recommendation is that the Maximum jobs per client be set at a higher value. Our suggested setting is 10. If a lower value is required for certain storage units, restrict the **Limit jobs per policy** setting in the backup policies for these Storage Units.

The next figure shows the **Global Attributes** settings on a test system. In the example, the **Maximum jobs per client** has been updated to 10.



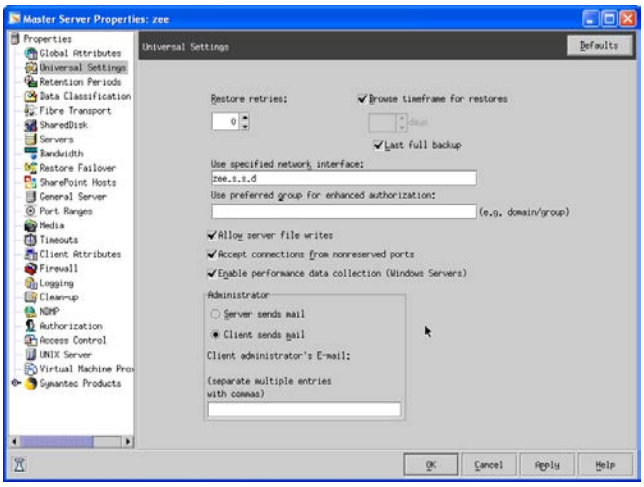
Global Attributes Settings on a Test System

5. Click **OK.**
6. Select **Universal Settings** in the **Properties** menu.

The next figure shows the **Universal Settings** for a master server zee. The **Restore retries** value allows the NetBackup administrator to select and implement the retry count for Restore jobs. By default, the value is 0.

Note

The Host Properties settings within NetBackup are robust. Therefore, the NetBackup administrator can configure the host properties for one master server, media server or client without effects on the other servers or clients in the NetBackup environment.



Universal Settings Example for a Master Server zee

Configuration and Use of Logs in Troubleshooting

This section describes how to configure logs and provides an example of how to use logs during a basic debug process.

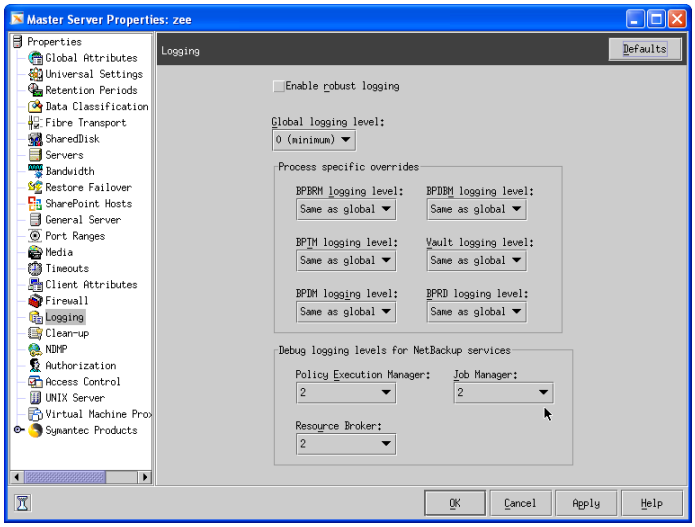
Log Configuration

When detailed logging is required, consult Veritas's Support Engineer to determine the correct logging levels to implement for all NetBackup services.

⚠ CAUTION

Setting the log levels of any NetBackup services may require NetBackup services to be stopped and restarted. In addition, to enable detailed logging without the proper procedures in place to monitor and remove logs as they accumulate could cause logs to consume all available disk on the system.

The next figure shows the default logging parameters for master server **zee**.



Default Logging Parameters for NetBackup Master Server zee

A NetBackup system has two types of logs: unified logs and the legacy NetBackup logs.

1. Unified logs are located in the *NetBackup_install_path*->logs directory. Refer to the *Veritas NetBackup Troubleshooting Guide for Unix and Windows* on how to use the vxlogview command to view NetBackup's Unified logging entries. You can obtain NetBackup examples of viewing unified log entries from: https://www.veritas.com/support/en_US/article.100017099.html.
2. Legacy logs are located in *NetBackup_install_path*->netbackup->logs directory. Run the mklogdir command to create the legacy log folders.

The following procedures describe how to configure the logs, view unified logs, and provide a basic example of how to use the logs in troubleshooting.

Not all NetBackup/Data Domain integration issues are as simple to debug as the one shown in the example. The example shows logical steps for review of NetBackup logs, but the example may not replace the need for Data Domain engineering analysis or the support of Veritas TSA net.

Configure Logging

Procedure

1. From the left menu of the NetBackup console, select **Host Properties**.
2. Select **Master Servers** and select the host on the right pane of the NetBackup console.
3. Right click and select **Properties.**
4. Select **Logging** and tune the logging parameters as desired.

View Unified Logs

Procedure

1. Go to the *NetBackup_install_path*->netbackup->bin directory.

cd *NetBackup_install_path*/netbackup/bin

2. Enter the `vxlogview` command with the following options:

`vxlogview -p 51216 -X jobid=N > N.log`

In the following example, the job ID is 1. The redirect (>) pipes the log results to an output file named `1.log` for debugging purposes.

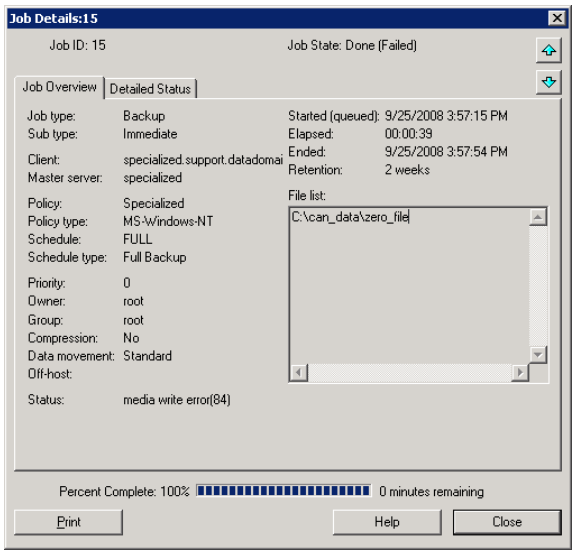
`vxlogview -p 51216 -X jobid=1 > 1.log`

Debug a NetBackup Failed Job (Example)

Procedure

1. Select the Job Details for the failed job and find out when the first error occurred.

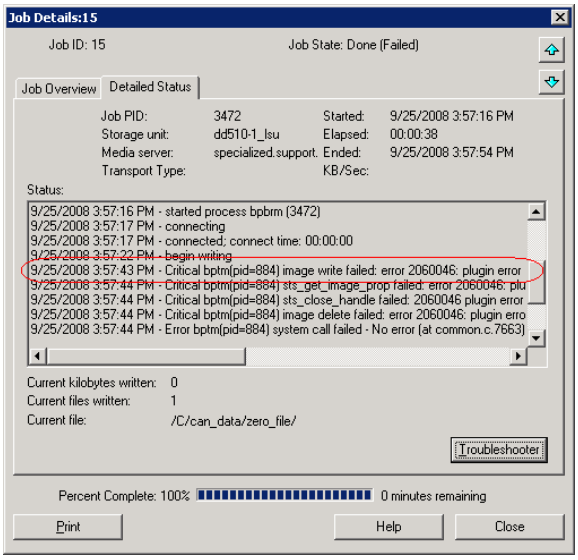
   The next figure shows Job Details for a failed backup. The Status field on the Job Overview tab indicates the job failed with `media write error(84)`.



Job Details for a Failed Job

2. Select the Detailed Status tab and look for the plugin error.

   The Detailed Status tab shows excerpts from the `bptm.log` file. The first error message (highlighted in the next figure) is `Critical bptm(pid=884) image write failed with a plugin error`.



Detailed Status Example

3. Review the `bpdm.log`.

   The example excerpt from the `bpdm.log` file shows that the backup failed because OST is not enabled.

   ```
   15:57:48.984 [324.296] <16> dd510-1.support.datadomain.local: C:\Program
   Files\Symantec\NetBackup\bin\\ost-plugins\libstspi
   DataDomain.dll:stspi_get_server_prop STS_EPLUGIN ost get property failed:
   not enabled (nfs: Permission denied)
   ```

Performance Tuning

With Data Domain VTL, you can achieve the best global compression (deduplication ratio) with larger tape block sizes. By default, NetBackup uses a 64 KB block size. For performance tuning, refer to these Veritas Tech Notes:

Veritas Tech Notes

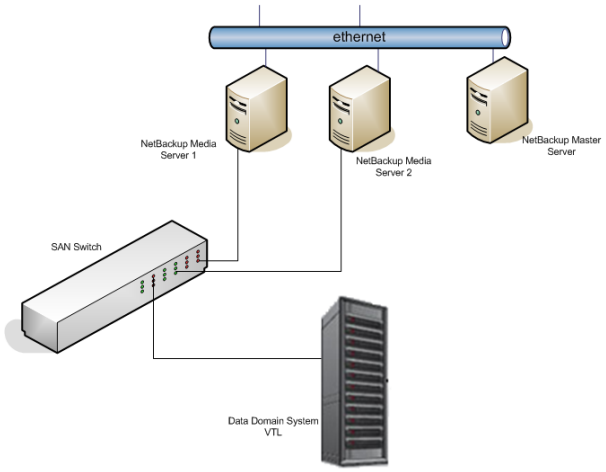
Operating System	URL for TechNote
UNIX	https://www.veritas.com/support/en_US/article.TECH1724
Windows	https://www.veritas.com/support/en_US/article.TECH18422
NDMP	https://www.veritas.com/support/en_US/article.TECH51967

The maximum tape block size that a given backup server or NAS filer can use depends on its architecture. Performance usually increases with larger block sizes, but depends on several different system features. To get the best performance, you need to experiment with different block sizes.

When you share a library with several systems, be sure to use a tape block size that all of the systems support. Otherwise, you will not be able to restore a tape to an alternate server.

NetBackup SSO Configuration

Shared Storage Option (SSO) is a NetBackup feature that allows tape drives to be shared between multiple NetBackup media servers. When you set up SSO, make sure all NetBackup media servers are within the same SAN zone. The next figure shows an example configuration of a Data Domain VTL with one NetBackup master server and two NetBackup media servers that are connected to a SAN switch. On the SAN switch, the NetBackup media servers are zoned with the same Data Domain system VTL.



NetBackup SSO Configuration With a Data Domain VTL

Set Up an SSO Configuration

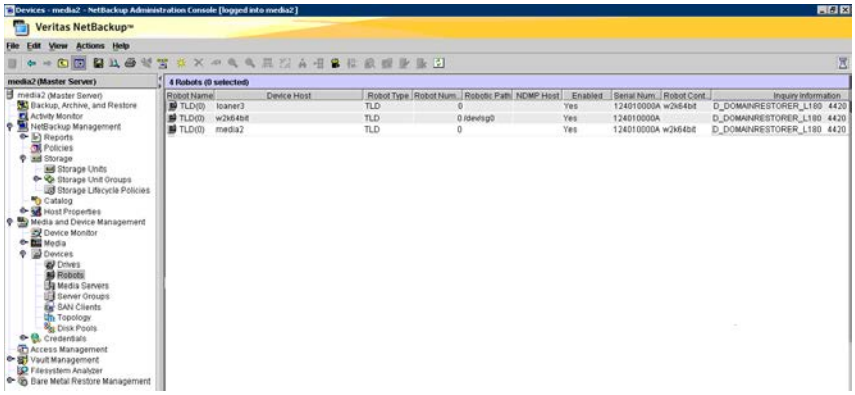
About this task

Following are the basic requirements for an SSO set up.

Procedure

1. Make sure a NetBackup SSO license is installed on the NetBackup master server and on all the NetBackup media servers that share the VTL.
2. Verify that the correct tape device and changer drivers are loaded for all the platforms.
3. Verify that all the media servers detect the VTL and the tape drives that are going to be set up for SSO.

The next figure shows how a Data Domain system VTL that is shared in the SSO environment is presented from the NetBackup console's Media and Device Management window.



SSO—Shared Data Domain System VTL

After you finish

For Veritas-recommended device configuration techniques and troubleshooting tips for tape library configuration, see the *Veritas NetBackup Device Configuration Guide*.

Data Domain Replication Configuration and Restoration

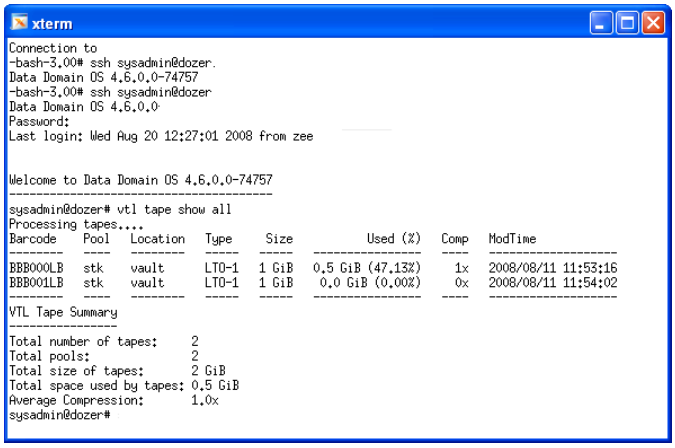
Data Domain replication types are collection replication and directory replication.

Collection replication replicates the complete `/backup` directory from one Data Domain system to another Data Domain system.

Directory replication is more granular. It allows for replication at the individual directory level.

Restoration of VTL Volumes from a Replica

To restore backups from VTL volumes from a Data Domain system replica, existing volumes in the current VTL must be exported out of the current VTL library. In a physical tape library, the physical tape volume is exported out from one physical tape library, moved and imported into another physical tape library. With VTL the export and import processes are non-physical. Virtual tape volumes that are exported out of a VTL tape library are put into a virtual vault. The next figure shows virtual tape volumes that are now in the vault location.



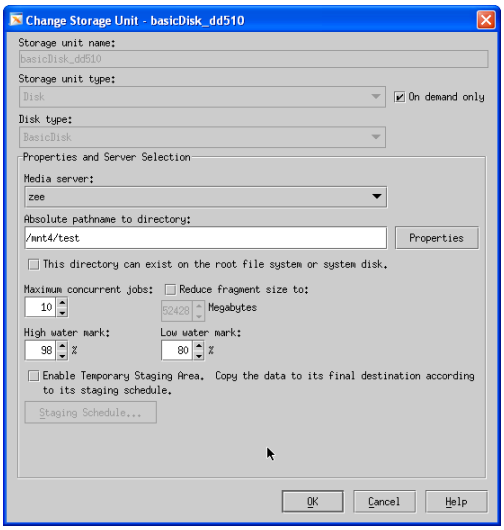
Exported Virtual Tape Volumes in a Vault

Once the volumes are exported to the vault, the volumes that were replicated to the secondary Data Domain system must then be imported into the new VTL library.

Restoration of a Replica Configured as a BasicDisk Storage Unit

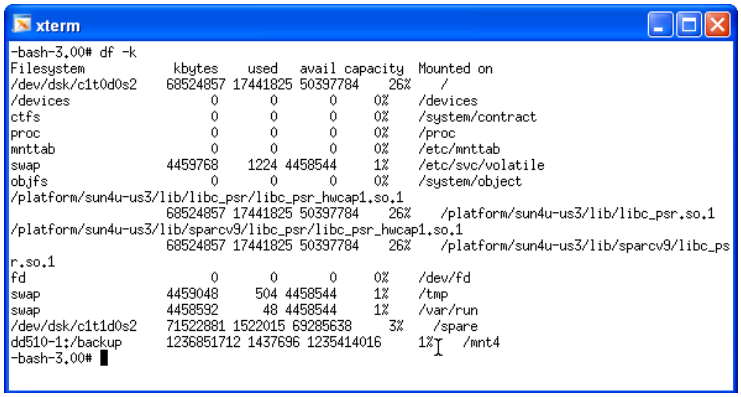
Restore from a Data Domain system replica configured as a BasicDisk Storage Unit is not straightforward because NetBackup does not know that replication has taken place and that an alternative device is available. The following is an example of how to execute a restore from a Data Domain system replica from the same Solaris NetBackup media server.

The next figure shows the Absolute pathname to directory for the Storage Unit `basicDisk_dd510` is `/mnt4/test`.



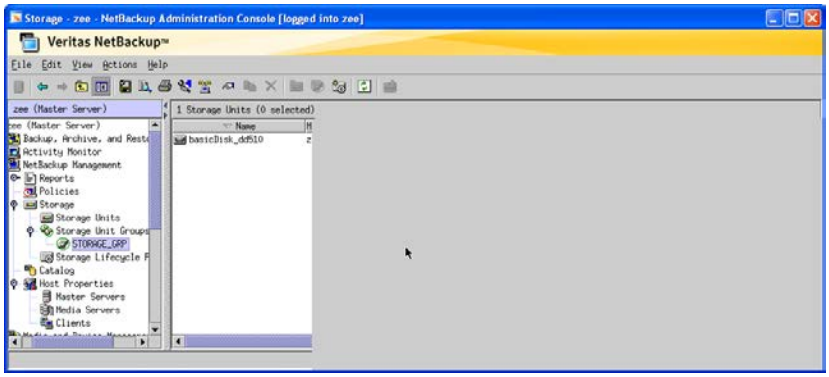
Storage Unit `basicDisk_dd510` with `/mnt4/test` Backup Destination

The next figure shows `dd510-1:/backup` is mounted on `/mnt4`.



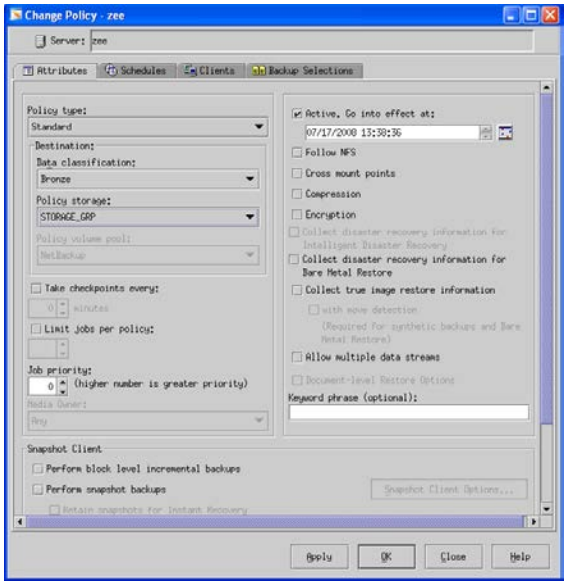
`dd510-1:/backup` Mounted to `/mnt4`

The next figure shows that STORAGE_GRP contains `basicDisk_dd510` Storage Unit.



STORAGE_GRP Contains `basicDisk_dd510` Storage Unit

The next figure shows NetBackup backup policy zee uses the Storage Group STORAGE_GRP which contains the `basicDisk_dd510` Storage Unit.



Backup Policy zee With STORAGE_GRP as the Policy Storage

Backup policy zee is executed and backup completes successfully with the STORAGE_GRP policy.

Configure Replication on the Data Domain System

Procedure

1. Log into a Data Domain System Manager Web console.
2. Verify that the replication license exists.
3. Configure replication as described in the Data Domain Operating System User Guide.

The next figure shows an example of directory replication on a Data Domain system. In the example, the source (primary Data Domain system) is dozer.d.d.l, the destination (secondary Data Domain system) is dd510-1.

Directory Replication on a Data Domain System

Import Volumes Into a New VTL Library

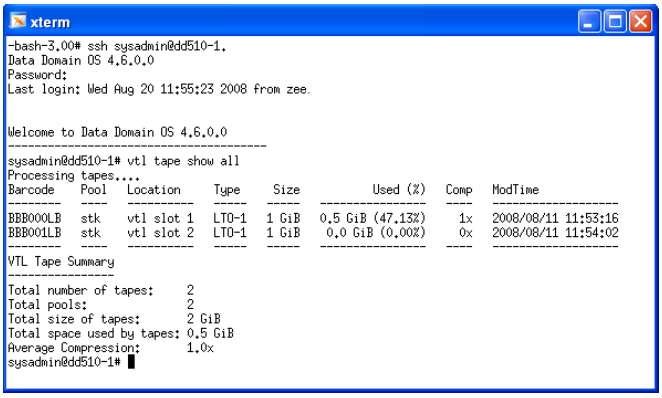
Procedure

On the command line of the secondary Data Domain system, run the `vtl import` command with the following syntax:

`vtl import` *`vtl_name`* `barcode` *`barcode`* `[count` *`count`*`] [pool` *`pool_name`*`] [element` *`drive`* `|` *`cap`* `|` *`slot`*`] [address` *`addr`*`]`

Results

The next figure shows replicated VTL tape volumes from the secondary Data Domain system that have been imported into the new tape library named vtl.



Replicated VTL Tape Volumes in the vtl Tape Library

Restore a VTL from a Secondary Data Domain System

Procedure

1. Export the VTL tape volume(s) from the current VTL. Use NetBackup to export the volume(s). For example, export BBB000 volume from NBU.
2. From the current DDR, execute `vtl export` to export the volume(s) to the vault location with the following syntax:

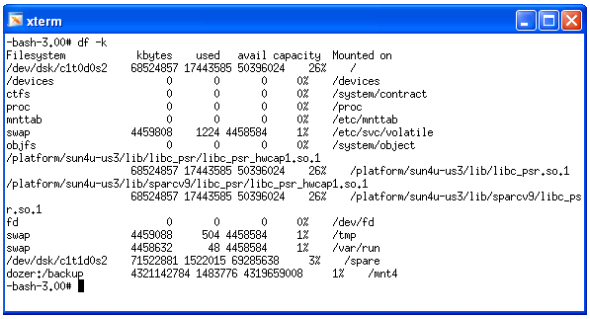
   `vtl export` *`vtl`* `slot` *`address`* `count` *`count`*
3. From the replica DDR, execute `vtl import`, to import the volume(s) into the replica VTL with the following syntax:

   `vtl import` *`vtl`* `barcode` *`barcode`*`sysadmin#dd510-1#` **`vtl import vtl2 barcode BBB000`**
4. Execute a NetBackup inventory to update the replica VTL with the imported volumes.
5. Backup images can be recovered from the write-protected replica VTL volume.

Restore from a Replica Data Domain System

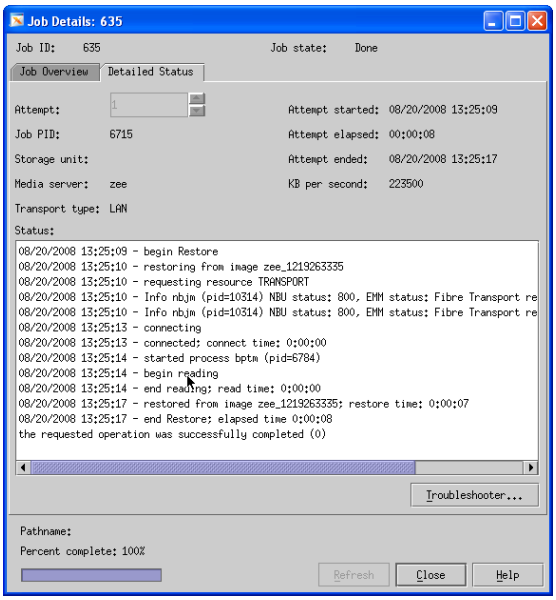
Procedure

1. Before you attempt to restore from a replica Data Domain system, verify that Data Domain replication has been synchronized. For example, the `df -k` command output on a UNIX media server in the next figure shows that `/mnt4` has been remounted with the secondary Data Domain system path.



/mnt4 Remounted With the Secondary Data Domain System

2. Execute a restore of the backed up image. The next figure shows a successful restore of a backup from the secondary Data Domain system from the same Solaris NetBackup media server.



Restore from a Secondary Data Domain System

Restore from a Secondary Data Domain System

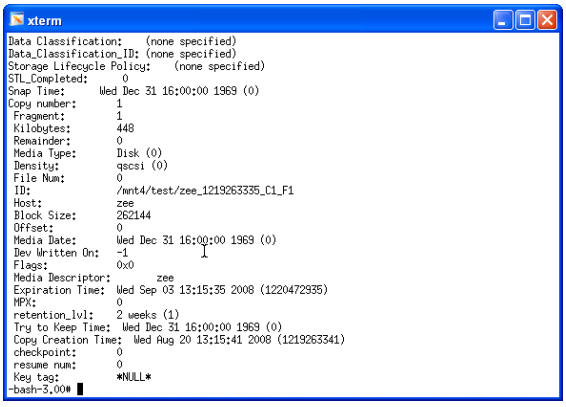
About this task

This procedure describes how to restore from a secondary Data Domain system connected to a different NetBackup media server. The mount point is shown as `/mnt4` in the examples of how to mount the secondary Data Domain system on the NetBackup media server #2. The NetBackup commands swap the backup image for restore from a different server.

Procedure

1. Go to the *`NetBackup_install_path`*`->netbackup->bin->admincmd` directory.
2. Execute the command `bpimagelist -L` to view the backed up images.

3. Identify the backup image to be restored. For example, the next figure identifies an image to be restored.



Backed up Image Identified by the Backup ID

4. Specify the image to be restored from the second media server. Run the `bpimage` command with the following syntax:

```
bpimage -newserver new_server_address -oldserver old_server_address -
id image_filename
```

Note

The image file specified with the `-id` option must be available for restore from the second media server.

The following example specifies that the backup image `zee_121926335_C1_F1` should be restored from media_server2.test.local instead of media_server1.test.local

```
-bash-3.00# bpimage -newserver media_server2.test.local -oldserver
media_server1.test.local -id zee_121926335_C1_F1
```

Tape Block Size Optimization

NetBackup uses a default tape block size of 64 KB. Larger tape blocks generally provide better performance (because there are fewer I/O commands therefore less overhead) as well as better compression within the Data Domain system. You may increase the size of the blocks that NetBackup writes to tape by creating a file called `SIZE_DATA_BUFFERS` with the size desired in bytes (for example, 524288 for 512 KB). This file must be placed in the *`NetBackup_install_path`*`/netbackup/db/config` directory.

Note

There is no warning if you place the file in the wrong directory or name it incorrectly. Verify that the new block size is in effect by checking details of the activity log for the job. In the example below, the message `using 524288 data buffer size` indicates that NetBackup recognized the changed block size.

```
10/17/2013 6:32:28 AM - Info bpbkar32(pid=5280) Backup started
10/17/2013 6:32:28 AM - Info bpbkar32(pid=5280) change time
comparison:<disabled>
10/17/2013 6:32:28 AM - Info bpbkar32(pid=5280) archive bit
processing:<enabled>
10/17/2013 6:32:28 AM - Info bpbkar32(pid=5280) not using change journal data
```

```
for <C:\comp_data>: not enabled
10/17/2013 6:32:28 AM - Info bptm(pid=5428) start
10/17/2013 6:32:29 AM - Info bptm(pid=5428) using 524288 data buffer size
10/17/2013 6:32:29 AM - Info bptm(pid=5428) setting receive network buffer to
2098176 bytes
10/17/2013 6:32:29 AM - Info bptm(pid=5428) using 30 data buffers
10/17/2013 6:32:29 AM - Info bptm(pid=5428) start backup
10/17/2013 6:32:29 AM - Info bptm(pid=5428) Waiting for mount of media id
G000L4 (copy 1) on server win-qnhrsvcoeiq.
10/17/2013 6:32:29 AM - mounting G000L4
```

Changing block size is not necessary, although it may improve performance. Some warnings are in order:

- Larger block size does not always improve throughput. It is suggested to make comparisons with the default NetBackup block size. Since larger tape blocks require the operating system to set aside more physical memory, that memory is unavailable for other processes therefore possibly causing lower backup performance.
- Most, but not all operating systems can handle large tape block sizes. Some notable examples are:
    - HP-UX prior to 11v3 (11.31) has a maximum tape block size of 256 KB.
    - On older versions of Solaris if the tape driver configuration file (`st.conf`) is not edited properly for the tape drive, the maximum block size will be 64 KB.
    - Some Fibre Channel HBAs limit the maximum block size. For example, Emulex HBAs on Windows are currently limited to 512 KB.
    - Certain HBAs on some Linux operating systems fail when attempting to write large blocks. If backups (with a `SIZE_DATA_BUFFERS` file created for large blocks) fail, but it is possible to label tapes with NetBackup, this may be the reason. For more information about this issue, and instructions for specifying a parameter for the HBA driver that will allow large blocks, see the EMC Data Domain Knowledge Base articles *VTL: Read/Write Issues with Initiators and Emulex FC HBAs* (document ID 92370) and *VTL: Read/Write Issues with Initiators and Brocade FC HBAs* (document ID 94841). Both articles are available on support.emc.com

With Solaris and HP-UX, if the HBA driver is unable to write the larger block size specified in `SIZE_DATA_BUFFERS`, it will silently write multiple blocks. NetBackup will fail at the end of a backup and report this error: `Media Write error, too many blocks`. If this error is encountered, revisit `st.conf` if using Solaris. It may be necessary to reduce the block size specified in `SIZE_DATA_BUFFERS`.

For NDMP backups it is also possible to write larger blocks than the NetBackup default of 64 KB. Rather than specifying the NDMP tape blocksize in file `SIZE_DATA_BUFFERS`, the file name is `SIZE_DATA_BUFFERS_NDMP`. However, note these issues:

- Many NDMP filers, such as NetApp, have a maximum tape block size of 256 KB. NetBackup will fail when attempting to use larger block sizes.
- EMC Celerra/VNX by default has a maximum NDMP tape block size of 128 KB. You can increase the maximum by setting the VNX PAX parameter `readWriteBlockSizeInKB`

- to 256 and also VNX NDMP parameter `bufsz` to at least 256. 256 KB is the absolute maximum NDMP tape block size for VNX. For more information refer to the EMC document Configuring NDMP Backups on VNX available at support.emc.com