

CommVault® Galaxy™

Client Installation and Administration Guide
(NetApp NAS NDMP)

Software Version 4.2.0
D-DA-W-NA-ADMIN Rev. 8

Dynamic Data Management™

Data & Storage Management Software



Copyright

© 2001-2003 by CommVault Systems, Inc. All rights reserved.

The information in this document is subject to change without notice. CommVault Systems assumes no responsibility for any errors that may appear in this document. No part of this document may be reproduced in any form or by any means - graphic, electronic or mechanical, including photocopying, recording, taping, or storage in an information retrieval system - without prior written permission of the copyright owner.

Trademarks

CommVault, CommVault Systems and logo, QiNetix, CommVault Galaxy and design, CommCell, CommNet, CommServe, CommServe StorageManager, *iDataAgent*, MediaAgent, and Storage without Boundaries, are trademarks and, in certain jurisdictions, may be registered trademarks of CommVault Systems, Inc.

NetApps is a registered trademark of Network Appliance, Inc.

Microsoft, Windows, Windows NT and Windows 2000 are trademarks or registered trademarks of Microsoft Corporation.

InstallShield and UnInstallShield are registered trademarks of InstallShield Software Corporation.

Any other trademarks appearing in this document are the property of their respective owners.

CommVault Systems, Inc.
End User License and Limited Warranty Agreement

CommVault® Software Release 4.2.0
(including Microsoft® SQL Server™ 2000)

End User License Agreement

IMPORTANT- READ CAREFULLY: THIS END USER LICENSE AGREEMENT (“EULA”) IS A LEGAL AGREEMENT BETWEEN YOU (EITHER AS A SINGLE INDIVIDUAL OR ENTITY) AND COMMVAULT SYSTEMS, INC. (“COMMVAULT”) FOR THE SOFTWARE PRODUCT(S) IDENTIFIED HEREIN, WHICH INCLUDES COMPUTER SOFTWARE AND MAY INCLUDE ASSOCIATED MEDIA, AND “ONLINE” OR ELECTRONIC DOCUMENTATION (“SOFTWARE”). BY INSTALLING, COPYING OR OTHERWISE USING THE SOFTWARE, YOU AGREE TO BE BOUND BY THE TERMS OF THIS EULA. IF YOU DO NOT AGREE TO THE TERMS OF THIS EULA, DO NOT INSTALL OR USE THE SOFTWARE; YOU MAY, HOWEVER, PROMPTLY RETURN THIS PACKAGE TO YOUR PLACE OF PURCHASE FOR A FULL REFUND. YOU SHALL INFORM ALL USERS OF THE SOFTWARE OF THE TERMS AND CONDITIONS OF THIS EULA.

This EULA, grants you, the user, a non-exclusive license to use the Software under the terms and conditions stated herein. You agree that all upgrades, enhancements, maintenance releases, patches, bug-fixes or other modifications to the Software provided to you shall be governed by the terms and conditions, including the limited warranty, exclusive remedies and limitations of liability provisions, contained in this EULA. The license granted herein shall be perpetual provided you comply with the terms hereof. This EULA shall be in effect until terminated. You may terminate this EULA at any time by destroying all copies of Software and corresponding documentation. This EULA will terminate immediately without notice from CommVault if you fail to comply with any provision of this EULA. Upon termination, you must destroy all copies of Software in your possession or control.

You may: (i) use the Software, with the same or lower version number identified herein, in numbers equal to the number of licenses purchased for all items; (ii) make copies of the Software, documentation or other user information accompanying the Software solely for back-up purposes, provided such back-up copies are only utilized as a replacement for the original copy on the same computer that the Software was previously installed; and, (iii) make a copy or print documentation provided in electronic form. You must incorporate all copyright and other notices included on the materials on any copies or partial copies that you make.

You may not: (i) make a copy of any of the Software for any purpose not explicitly permitted herein; (ii) sell, sublicense, rent, loan or lease the Software to another party, without the prior written consent of CommVault; (iii) except to the extent that such a prohibition is expressly prohibited by law, decompile, disassemble, reverse engineer or modify, in any manner, any of the Software; (iv) transfer or assign your rights to use the Software; or, (v) use the Software for any purpose other than as permitted in this EULA.

If the Software is provided to you for demonstration, test or evaluation purposes or is labeled “Not for Resale,” then, notwithstanding anything to the contrary in the EULA, your use of the Software is limited to use for demonstration, test or evaluation purposes, and you may not resell or otherwise transfer the Software. With respect to any technical information you provide to CommVault as part of any demonstration, evaluation, beta, or support service, you agree that CommVault may collect, process and use such information for its business purposes, provided that such information does not personally identify you.

All title and intellectual property rights in and to the Software, and any copies you are permitted to make herein, are owned by CommVault and/or its licensors and is protected by United States and other country copyright, trade secret, and other laws and by international treaty provisions. **This Software is licensed, not sold.** CommVault and/or its licensors retain ownership of the Software. No rights are granted to you other than a license to use the Software upon the terms expressly set forth in this EULA. Such licensors, in addition to any other rights or remedies available to them, are third party beneficiaries of this EULA for their respective software and may have the right to enforce such terms against you. The structure, sequence, organization and source code of the Software are valuable trade secrets of CommVault and/or its

licensors. The export of the Software may be restricted by the export control laws of the United States of America and other countries. You agree to comply strictly with all such regulations and acknowledge that you have the responsibility to obtain licenses to export, re-export, or import Software. This EULA shall be governed by the laws of New Jersey, USA, without regard to any provisions concerning the applicability of the laws of other jurisdictions. This EULA is the complete and exclusive statement of your agreement with CommVault with respect to the subject matter hereof and supersedes all prior agreements. If any provision of this EULA is held to be invalid or unenforceable by a court of competent jurisdiction, the remaining provisions of this EULA shall remain in full force and effect.

All rights not expressly granted hereunder are expressly reserved by CommVault.

Note on JAVA Support

THIS SOFTWARE PRODUCT MAY CONTAIN SUPPORT FOR PROGRAMS WRITTEN IN JAVA. JAVA TECHNOLOGY IS NOT FAULT TOLERANT AND IS NOT DESIGNED, MANUFACTURED, OR INTENDED FOR USE OR RESALE AS ONLINE CONTROL EQUIPMENT IN HAZARDOUS ENVIRONMENTS REQUIRING FAIL-SAFE PERFORMANCE, SUCH AS IN THE OPERATION OF NUCLEAR FACILITIES, AIRCRAFT NAVIGATION OR COMMUNICATION SYSTEMS, AIR TRAFFIC CONTROL, DIRECT LIFE SUPPORT MACHINES, OR WEAPONS SYSTEMS, IN WHICH THE FAILURE OF JAVA TECHNOLOGY COULD LEAD DIRECTLY TO DEATH, PERSONAL INJURY OR SEVERE PHYSICAL OR ENVIRONMENTAL DAMAGE. Microsoft Corporation obligated CommVault to make this disclaimer.

Limited Warranty

CommVault warrants that the Software licensed hereunder shall be new and shall operate substantially in accordance with its user documentation for a period of ninety (90) days from the date of shipment by CommVault (hereinafter the "Warranty Period"). If, during the Warranty Period, you believe any Software product to be defective, you must immediately notify CommVault in writing and follow CommVault's instructions regarding the return of such Software product. CommVault's sole liability to you, and your sole remedy, shall be, at CommVault's option, (i) repair or replacement of the Software product which does not comply with this Limited Warranty, or (ii) return of the amount paid by you for the Software product which does not comply with the Limited Warranty. In the event CommVault determines that the software product is in compliance with this Limited Warranty, you shall pay the cost of all charges associated with the inspection and shipment of such Software product by CommVault.

Limited duration licenses, site licenses, beta, evaluation, test or demonstration Software products are delivered "AS IS" without a warranty of any kind.

Disclaimer. COMMVAULT DOES NOT WARRANT THAT THE SOFTWARE WILL OPERATE UNINTERRUPTED OR ERROR FREE. THIS LIMITED WARRANTY PROVIDED HEREIN IS IN LIEU OF ALL OTHER WARRANTIES. COMMVAULT DISCLAIMS ALL OTHER WARRANTIES, EXPRESS OR IMPLIED, EITHER IN FACT OR BY OPERATION OF LAW, STATUTORY OR OTHERWISE, AND COMMVAULT EXPRESSLY EXCLUDES AND DISCLAIMS ANY WARRANTY OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, SATISFACTORY QUALITY, AND NONINFRINGEMENT OF INTELLECTUAL PROPERTY RIGHTS. THE PROVISIONS SET FORTH ABOVE STATE COMMVAULT'S ENTIRE RESPONSIBILITY AND YOUR SOLE AND EXCLUSIVE REMEDY WITH RESPECT TO ANY BREACH OF ANY WARRANTY.

No Consequential Damages. NEITHER COMMVAULT, NOR ANY OF ITS LICENSORS, WILL, UNDER ANY CIRCUMSTANCES, BE LIABLE TO YOU OR ANY OTHER PARTY, FOR COSTS OF PROCUREMENT OF SUBSTITUTE PRODUCTS OR SERVICES, LOST PROFITS, LOSS OF INFORMATION OR DATA OR ANY OTHER SPECIAL, INDIRECT OR CONSEQUENTIAL DAMAGES, REGARDLESS OF THE FORM OF ACTION ARISING OUT OF OR RELATING TO THIS LIMITED WARRANTY OR RESULTING FROM THE LICENSE OF SOFTWARE PRODUCTS OR USE BY YOU OR ANY OTHER PARTY OF SUCH PRODUCTS, EVEN IF COMMVAULT OR ANOTHER PARTY HAS BEEN NOTIFIED OF THE POSSIBILITY OF SUCH DAMAGES AND NOTWITHSTANDING ANY FAILURE OF AN ESSENTIAL PURPOSE OF THIS LIMITED WARRANTY.

Limit of Liability. **IN THE EVENT COMMVAULT IS SUBJECT TO ANY LIABILITY IN CONNECTION WITH THE SOFTWARE PRODUCTS, WHETHER ARISING FROM NEGLIGENCE, BREACH OF CONTRACT OR OTHERWISE, COMMVAULT'S LIABILITY WILL NOT EXCEED THE SUM PAID BY YOU TO COMMVAULT FOR THE SOFTWARE PRODUCT WHICH WAS FOUND TO HAVE NOT COMPLIED WITH THIS LIMITED WARRANTY. THIS LIMITATION SHALL APPLY EVEN IF COMMVAULT HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES AND NOTWITHSTANDING ANY FAILURE OF ESSENTIAL PURPOSE OF ANY LIMITED WARRANTY.**

These terms and conditions, warranties, limitations and remedies contain an allocation risk between you and CommVault. Accordingly, CommVault's prices reflect such allocation of risk. Because some jurisdictions restrict the ability to exclude implied warranties, limit or exclude incidental or consequential damages or limit liability, the foregoing limitations and exclusions may not apply to you.

United States Government and DOD

This article applies to all acquisitions of this Software by or for the Federal Government. By accepting delivery of this Software, you hereby agree that this software qualifies as "commercial computer software" as that term is used in the acquisition regulation(s) applicable to this procurement. The terms and conditions of this EULA shall pertain to the Government's use and disclosure of this Software, and shall supersede any conflicting contractual terms and conditions. If this EULA fails to meet the Government's minimum needs or is inconsistent in any respect with Federal procurement law, the Government agrees to return this software, unused, to CommVault.

Trademark Acknowledgment

CommVault, CommVault Systems and logo, QiNetix, CommVault Galaxy and design, Storage without Boundaries, CommServe, CommServe StorageManager, MediaAgent, iDataAgent, CommCell and CommNet are trademarks, and may be registered trademarks, of CommVault Systems, Inc.

Patent Acknowledgment

This Software is covered by US Patent Numbers 5,559,991; 5,642,496 and 6,418,478 and other patents pending.

Copyright Acknowledgment

© 1997-2003 CommVault Systems, Inc. All rights reserved.

Contents

1 **iDataAgent Installation**

iDataAgent Deployment Flowchart	1-2
Terminology	1-3
System Requirements	1-4
Windows	1-4
Unix	1-6
Verify Hardware Installation	1-8
Verify Installation of Prerequisite QiNetix Components	1-10
Windows	1-10
Unix	1-10
Installing the iDataAgent	1-11
Installing the MediaAgent and NetApp NAS NDMP iDataAgent on Windows Platforms	1-12
Installing the iDataAgent on a Unix Platform	1-16
Installing the NDMP Remote Server (NRS) on a Unix MediaAgent	1-19
Post-Install Considerations	1-22
Configuring Libraries and Drives for NetApp NAS NDMP iDataAgent	1-23
Configuring the Library and Drives Attached to a NetApp filer	1-23
Configuring Stand-alone Drives attached to a NetApp filer	1-39
Configuring a Library Attached to a MediaAgent and used by the NetApp NAS NDMP iDataAgent	1-45

Contents

Dynamic Drive Sharing (DDS) Between Multiple Devices in a SAN Environment	1-46
Adding Clients for NetApp NAS NDMP iDataAgents	1-51

2 System Overview

Introduction	2-2
Client Agents	2-3
Common Technology Engine	2-4
Qinetix Installations	2-6
What You Need to Know About the NetApp NAS NDMP iDataAgent	2-7
What You Need to Know About Galaxy	2-8
Subclients	2-9
NDMP Remote Server	2-12
Storage Policies	2-13
Copies	2-15
Archive Pruning	2-19
Hardware-Specific Resource Issues	2-21
Removable Media Libraries	2-21
Magnetic Disk Libraries	2-25
Backup Sets	2-27

3 Managing Your Data

Backup Overview	3-2
Full Backups	3-2
Incremental Backups	3-3
Differential Backups	3-4
When a Non-Full Backup is Automatically Converted to a Full Backup	3-5
Scheduled Backups	3-5
Backing Up Subclients and the Backup Set	3-7
Managing the Tapes Where the Data Resides	3-7

Excluding Data from Being Backed Up	3-8
Memsaver Option	3-9
Pre/Post User Impersonation for Backup Jobs	3-9
Backup Procedures	3-10
Restore Overview	3-14
Browsing Data	3-14
Restoring Data	3-14
Browse and Restore Scenarios	3-14
Browsing Multiple Versions of a File	3-21
Three-way Backup and Restore Operations	3-22
Cross-Client Restore Operations	3-23
File System NDMP Restore Operations	3-23
Direct Access Restore	3-24
Efficient Non-DAR Restore	3-24
Scheduled Restore Operations	3-25
Auxiliary Copy	3-25
List Media Operation	3-25
Restore Procedures	3-26

Contents

- A Removing the Galaxy Client Software**
- B Registry Keys and Parameters**
- C Upgrading the Galaxy Client Software**
- D Obtaining Information from the NetApp Filer**
- E NAS Disaster Recovery**
- F Enabling NDMP Service**
- G File System NDMP Restore Enabler**

Index

Preface

Revision History

The revision history of this manual is:

Revision	Date	Released with:*
6	March 2002	Software version 3.7.1
7	September 2002	Software version 4.1.0
8	March 2003	Software version 4.2.0

* This column identifies the software version that was current at the time the manual was created or revised. Unless superseded by a later revision, this manual applies to all future versions of the software as well.

This table does not necessarily list all previous manual revisions, only the most recent versions.



How to Use this Guide

This guide is intended for use by personnel responsible for the installation and/or administration of the CommVault® Galaxy™ NetApp NAS NDMP iDataAgent backup and recovery software.

Prior to installing any iDataAgent, we recommend you review the *CommCell Pre-Installation Checklist*, *CommServe Administration Guide*, and *CommCell Media Management Administration Guide* for information on planning the implementation of your QiNetix™ enterprise data management solution.

Conventions Used in this Document

The text in this manual observes the following conventions.

<code>Courier</code>	Identifies computer output, window options, user keys, file/directory names and paths.
Courier Bold	Identifies characters that should be typed as shown.
<i>Courier Italics</i>	Identifies variable information.
Required Capability:	Identifies the system capability that a user must have in order to perform a specific procedure.
 NOTE	Identifies a note, text containing special information, exceptions or unique conditions that affect the normal functioning of the product.
 CAUTION	Identifies a caution message, containing information about events or situations that could result in damage to system software or data.

Related Documentation

- ♦ *CommCell Pre-Installation Checklist*
- ♦ *CommCell Quick Start Guide*
- ♦ *CommCell Upgrade Guide*
- ♦ *CommServe Administration Guide*
- ♦ *CommCell Media Management Administration Guide*
- ♦ *Galaxy NetApp NAS NDMP iDataAgent Release Notes*
- ♦ *Galaxy Client Installation and Administration Guide (Windows File Systems)*
- ♦ *Galaxy Client Installation and Administration Guide (Unix File Systems)*

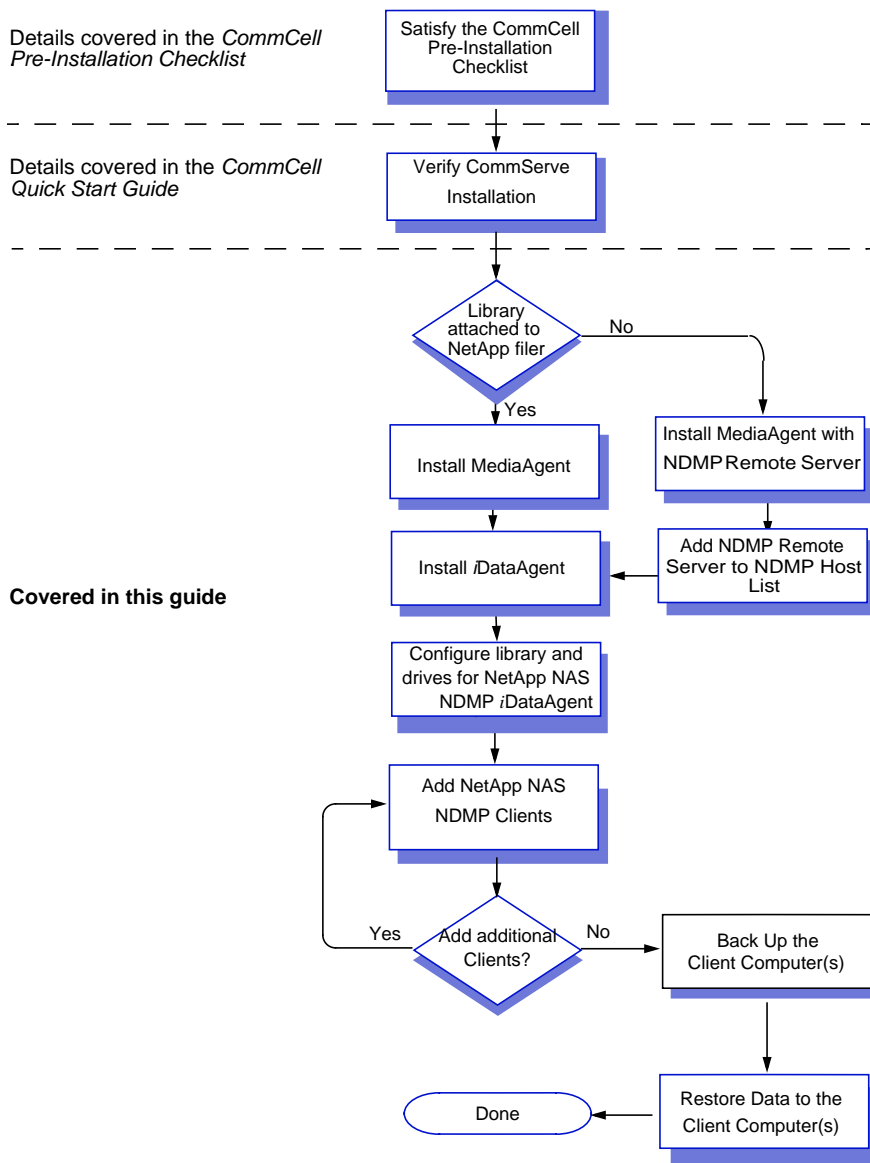
*i*DataAgent Installation

This chapter describes the NetApp NAS NDMP *i*DataAgent installation and configuration.

This chapter contains:

- ◆ iDataAgent Deployment Flowchart, 1-2
- ◆ Terminology, 1-3
- ◆ System Requirements, 1-4
- ◆ Verify Hardware Installation, 1-8
- ◆ Verify Installation of Prerequisite QiNetix Components, 1-10
- ◆ Installing the iDataAgent, 1-11
- ◆ Post-Install Considerations, 1-22
- ◆ Configuring Libraries and Drives for NetApp NAS NDMP iDataAgent, 1-23
- ◆ Adding Clients for NetApp NAS NDMP iDataAgents, 1-51

The following flowchart summarizes the major steps that you will undertake as you install and begin to use the NetApp NAS NDMP iDataAgent.



Terminology

Client refers to the NetApp filer on which the NetApp NAS NDMP iDataAgent secures data.

Install Program refers to the NetApp NAS NDMP iDataAgent installation program.

iDataAgent refers to the NetApp NAS NDMP iDataAgent. In this document, the NetApp NAS NDMP iDataAgent refers to the NAS NDMP iDataAgent component on a MediaAgent that performs data backup and recovery operations.

NDMP Remote Server refers to a component running on a MediaAgent that allows data from a NetApp filer to be backed up to a library attached to the MediaAgent computer. NDMP Remote Server also has all the functionality of the File System NDMP Restore Enabler.

File System NDMP Restore Enabler refers to the component running on any File System client that allows data from a NetApp filer to be restored to this File System client.

NDMP Server Device Name is the information from the NetApp filer on how to locate the media changer and drives associated with a library attached to that NetApp filer.

For information on the steps involved in obtaining the device name, see *Obtaining the Device Name of Media Changer* on page D-2.

NDMP Drive Access Path is the information from the NetApp filer used to locate the following:

- ♦ a specific drive
- ♦ the command set that must be used to access the drive

For information on the steps involved in obtaining a drive access path, see *Obtaining the Drive Access Path* on page D-3.

System refers to the QiNetix system.

System Requirements

Before you install, you need to ensure that your computers, resident software, and network can run and support the *iDataAgent*.

Requirements for the *iDataAgent* are as follows:

Windows

Computer/Processor

- ♦ See the requirements for the MediaAgent in the *CommCell Pre-Installation Checklist*.
- ♦ Additionally, 0.1% of the total backup size for the largest amount of data being backup up at any given time is recommended. (e.g., for 1 terabyte of backup data, you should have an additional 1 gigabyte of memory available.)

Memory

- ♦ See the requirements for the MediaAgent in the *CommCell Pre-Installation Checklist*.

Hard Disk

- ♦ 50 MB minimum of hard disk space for software
- ♦ 50 MB of additional hard disk space for log file growth
- ♦ 10 MB of temp space required for install or upgrade (where the temp folder resides)

The above mentioned requirements are beyond the requirements stated for the MediaAgent computer.

Operating System

- ♦ Microsoft Windows 2000 Advanced Server with Service Pack 2 or 3
- ♦ Microsoft Windows 2000 Server with Service Pack 2 or 3
- ♦ Microsoft Windows NT 4.0 Workstation with Service Pack 6a
- ♦ Microsoft Windows NT 4.0 Server with Service Pack 6a
- ♦ Microsoft Windows NT 4.0 Enterprise Server with Service Pack 6a

Application

The following software must be installed on the NetApp filer:

- ♦ ONTAP version 5.3.7 to 6.4.
 - To perform direct access restores, ONTAP 6.0 or higher is required
 - To support SAN attached libraries, ONTAP version 6.1 or higher is required
 - To perform incremental backups, 6.03D1 or 6.1.1 or higher is required
 - To perform direct access restores on directories, ONTAP version 6.4 or higher is required.

Peripherals

- ♦ CD-ROM drive
- ♦ Network Interface Card

Miscellaneous

- ♦ If tape drive(s) are attached to the NetApp NAS NDMP iDataAgent, one free SCSI or Fibre Channel port (of a supported type)
- ♦ If media changer and tape drives are attached to the filer, they must be of a type supported by NetApp
- ♦ Microsoft TCP/IP Services configured on the computer
- ♦ The MediaAgent will be automatically installed during installation of a NetApp NAS NDMP iDataAgent if it is not already installed. You will be prompted to install the Base software, if the installation software detects that you have not already installed the Base software.
- ♦ MediaAgent (Windows NT, Windows Server 2003 or Windows 2000 MediaAgent)



Due to the nature of the NetApp filer's operating system, the installation of the NetApp NAS NDMP iDataAgent differs from that of other iDataAgents. The NetApp NAS NDMP iDataAgent is installed to a server that contains a MediaAgent.

Unix

Computer/Processor

- ✦ See the requirements for the MediaAgent in the *CommCell Pre-Installation Checklist*.

Memory

- ✦ See the requirements for the MediaAgent in the *CommCell Pre-Installation Checklist*.
- ✦ Additionally, 0.1% of the total backup size for the largest amount of data being backup up at any given time is recommended. (e.g., for 1 terabyte of backup data, you should have an additional 1 gigabyte of memory available.)

Hard Disk

- ✦ 16 MB minimum of hard disk space for software
- ✦ 50 MB of additional hard disk space for log file growth
- ✦ 10 MB of temp space required for install or upgrade (where the temp directory resides)

The above mentioned requirements are beyond the requirements stated for the MediaAgent computer.

Operating System

- ✦ Solaris 2.6 32-bit
- ✦ Solaris 2.7 (Solaris 7) 32-bit
- ✦ Solaris 2.7 (Solaris 7) 64-bit
- ✦ Solaris 2.8 (Solaris 8) 32-bit
- ✦ Solaris 2.8 (Solaris 8) 64-bit

Peripherals

- ✦ CD-ROM drive
- ✦ Network Interface Card

Miscellaneous

- ✦ TCP/IP Services configured on the computer

- ♦ The MediaAgent will be automatically installed during installation of a NetApp NAS NDMP *iDataAgent* if it is not already installed. You will be prompted to install the Base software, if the installation software detects that you have not already installed the Base software.

Verify Hardware Installation

Follow the hardware configuration guidelines for the CommServe and MediaAgent indicated in the *CommCell Pre-Installation Checklist*.

For the NetApp NAS NDMP iDataAgent, the media changer and drives in a library can be attached to one or more of the following:

- ◆ The NetApp filer
- ◆ The MediaAgent
- ◆ Both the MediaAgent and/or NetApp filer(s) using a SAN network

For information on attaching the library to the NetApp filer, refer to the NetApp filer documentation.

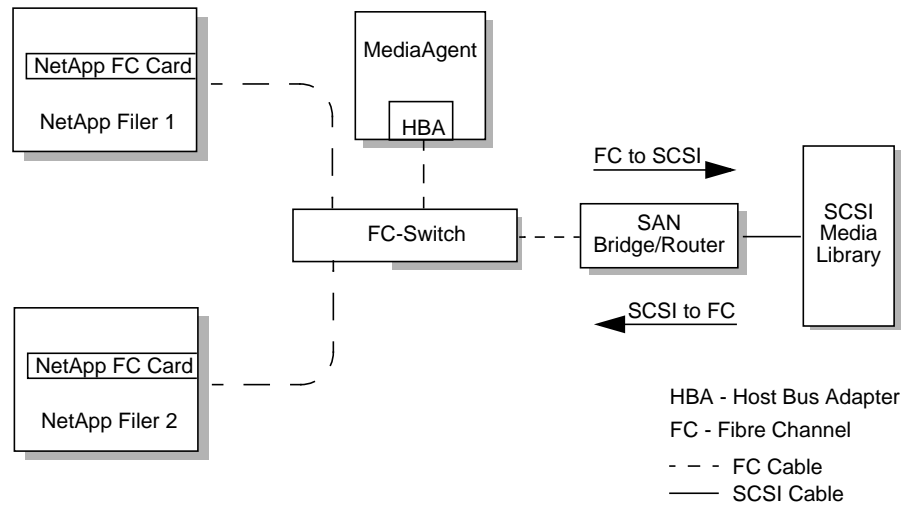
For information on attaching the library to the MediaAgent, refer to the *CommCell Pre-Installation Checklist*.

Observe the following guidelines if the library is attached to a SAN network.

NetApp filers can be connected to libraries through the Fibre Channel (FC) switch in a Storage Area Network (SAN). The FC switch allows multiple NetApp NAS NDMP iDataAgents to be connected to the drives in a library at the same time.

In the case of such NetApp NAS NDMP iDataAgents, the filer must contain a NetApp fibre channel card to allow it to communicate over a fibre channel connection to a fibre channel switch certified by Network Appliance. The library can communicate to the fibre switch through a bridge or fibre channel card.

The following is an example of a NetApp SAN configuration:



SAN Hardware Guidelines

You must follow the NetApp certification matrices configuration when you are setting up to use SAN. The hardware guidelines for a NetApp SAN configuration can be found at the Certification Matrices page on the NetApp web site (www.netapp.com).

Verify Installation of Prerequisite QiNetix Components

The iDataAgent can only be installed after the CommServe and at least one MediaAgent have already been installed in the CommCell. In addition, you must install the File System iDataAgent on the computer on which you plan to install the iDataAgent.

Although the File System iDataAgent is a prerequisite, you do not have to install it separately. For Windows, the NetApp NAS NDMP iDataAgent install program checks for the presence of the File System iDataAgent and installs it automatically if it is not installed. For system requirements and install information specific for File System iDataAgents, refer to the *Galaxy Client Installation and Administration Guide (Windows File Systems)* or the *Galaxy Client Installation and Administration Guide (Unix File Systems)*.

Also, keep in mind that the CommServe must be installed and running (but not necessarily on the same computer), before you can install the iDataAgent to the computer containing the MediaAgent.

This version of the iDataAgent is intended to be installed in a CommCell where the CommServe and all MediaAgents are a minimum software version 4.2.0.

Windows

This guide assumes that you have already installed the CommServe. For installation instructions, refer to the *CommCell Quick Start Guide*.

Since this iDataAgent is installed on the MediaAgent computer, the installation procedure on page 1-12 describes the steps involved in simultaneously installing the MediaAgent and NetApp NAS NDMP iDataAgent.

Unix

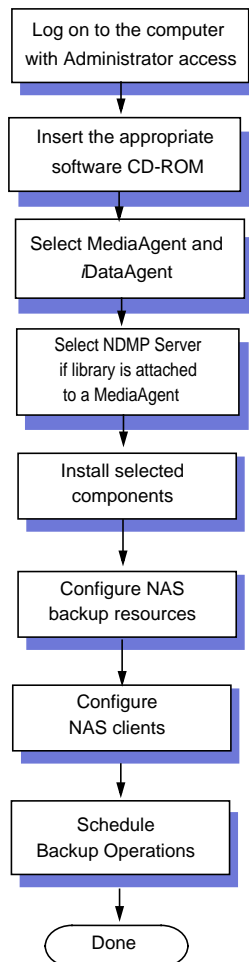
This guide assumes that you have already installed the CommServe, MediaAgent and File System iDataAgent.

If you have not already installed the CommServe and MediaAgent in the CommCell, do so now. For installation instructions, refer to the *CommCell Quick Start Guide*. For instructions on installing the File System iDataAgent, see the *Galaxy Client Installation and Administration Guide (Unix File Systems)*.

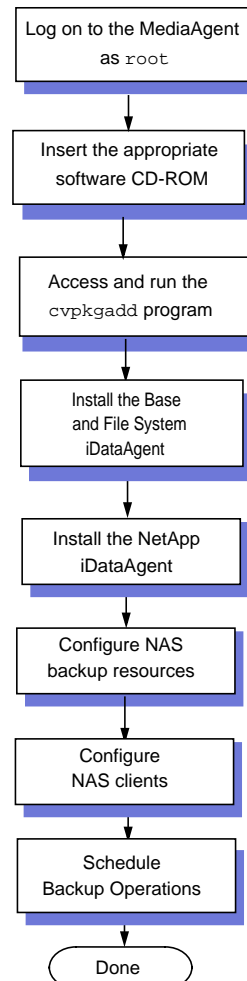
Installing the iDataAgent

Having satisfied the system requirements and checked for the prerequisite QiNetix components, you are ready to perform the install. For the NetApp NAS NDMP iDataAgent, the filer on which the files and folders reside is considered to be the client of the CommServe. The data on the client computer is accessed by the MediaAgent that contains the NetApp NAS NDMP iDataAgent. The following flowcharts illustrate the iDataAgent installation process(es).

iDataAgent Installation (Windows)



iDataAgent Installation (Unix)



Before You Begin

Review the following to avoid common problems:

- ◆ Close all applications and disable any programs that run automatically, including antivirus, screen savers and operating system utilities. Some of the programs, including many antivirus software, may be running as a service. Stop and disable such services before you begin. You can re-enable them after the installation.
- ◆ The client satisfies the minimum requirements provided in the *System Requirements* on page 1-4 for NetApp NAS NDMP iDataAgent system
- ◆ For the System Requirement for MediaAgent and File System iDataAgent, refer to the Pre-Installation Checklist.
- ◆ The CommServe is running.
- ◆ If your network does not have DNS lookup or some other name resolution facility, you may be asked to enter the IP address of the CommServe computer.
- ◆ If the CommServe, MediaAgent and/or Client are communicating across firewall(s), ensure that ports 8400 and 8402 are allowed connections through the firewall for these computers.
- ◆ Windows users will require a license on the CommServe for the MediaAgent and File System iDataAgent.

Installing the MediaAgent and NetApp NAS NDMP iDataAgent on Windows Platforms

The following steps describe an installation of the NetApp NAS NDMP iDataAgent on Windows NT, Windows 2000 or Windows Server 2003 platforms.

☐ To install the MediaAgent and iDataAgent on Windows platforms

Once you have reviewed *Before You Begin* on page 1-12, you are ready to install the iDataAgent.

- 1 Log on to the computer that will serve as the MediaAgent, as local Administrator or as a member of the local Administrators group on that computer.
- 2 Place the Galaxy Software CD-ROM into the CDROM drive. After a few seconds, the installation menu appears.

If the installation menu does not appear:

- a) Click `Start` on the Windows task bar, and then click `Run`.
- b) Browse the CD-ROM drive, right-click `Setup.exe` then click `Open`.
- 3 From the installation menu, click `Install QiNetix Software on this computer`.
- 4 From the `Welcome` dialog box, click `Next` to continue if no other applications are running.
- 5 Click `OK` to continue if virus scanning is disabled.
- 6 Read the license agreement. Select `I accept the terms in the license agreement` then click `Next` to continue.
- 7 From the `Select Platforms` dialog box, expand the `MediaAgent` module and select `MediaAgent` and select any applicable `MediaAgent` install options described below:

<code>NDMP Remote Server</code>	Select this option if your <code>MediaAgent</code> has a library attached and is used by a <code>NetApp NAS NDMP</code> client to backup data.
<code>iDA for NAS</code>	Select this option to install the <code>NetApp NAS NDMP iDataAgent</code> .

Click `Next` to continue.

- 8 If you previously installed any `QiNetix` components on this computer, you will not receive this prompt.

Select the location of the `Galaxy Destination Folder`. Either accept the default by clicking `Next` or use the `Browse` button to select a different location on a local disk drive. (Do not install the software to a mapped network drive.)



Do not use the following characters when specifying the `Galaxy` destination path:

`/ : * ? " < > | ! ; @ ^]`

It is recommended that you use alphanumeric characters only.

- 9 If this computer is your CommServe, you will not see this screen. Skip to the next step.

Enter the following information:

CommServe client name The local (NetBIOS) name of the CommServe computer.

CommServe host name The TCP/IP network interface name of the CommServe computer
(e.g., computer.company.com).

Click **Next** to continue.

- 10 You are prompted to select the MediaAgent's client name and interface name. Select the default interface name that backups/restores use to communicate with the MediaAgent.



You will be given a list of available host names for selection. If the host name is not complete or correct, check the network connection's working status. If necessary, type in the correct host name.

Click **Next**.

- 11 Select **Yes** and click **Next** to stop Remote Storage Services on the MediaAgent. This prompt will not appear if Remote Storage Services are already disabled on the target computer.
- 12 Select the location for the MediaAgent Index Cache. Accept the default or choose another location. In either case, the location must be local. Click **Next** to continue.
- 13 Specify whether the client is communicating with other components of the CommCell through a firewall.



If you are using NDMP Remote Server, you must specify port 10000.

- a) Enter the valid port ranges to the list and click **Next** to continue.
- b) Enter the host names or IP addresses of computers separated from this computer by the firewall. Click **Next** to continue.
- c) Enter a **Keep Alive** value, in minutes, to avoid TCP/IP timeouts through the firewall. Click **Next** to continue.

If the client is not communicating through a firewall, skip to the next step.

- 14** Specify the location of the client's job results directory. Accept the default or use the **Browse** button to specify a different location.

The install program creates the job results directory to store the client's backup and restore job results. Click **Next** to continue.

- 15** If you previously selected the option to install the MediaAgent as an NDMP server, provide the user name and password for NDMP remote server and click **Next** to continue.

- 16** A summary of the installation options that you have chosen appears. Click **Next** to continue or **Back** to change any option.

The install program now starts copying all agent software to the computer. This step may take several minutes to complete.

- 17** The system displays a dialog box asking if you want to configure a library attached to a MediaAgent. Click **Yes** or **No**.

- ♦ Click **Yes** if your MediaAgent has NDMP remote server. You can configure the libraries and drives as described in *Configuring a Library Attached to a MediaAgent and used by the NetApp NAS NDMP iDataAgent* on page 1-45 to finish your installation.
- ♦ Click **No** if your library is attached to a NetApp filer. Exit the Galaxy Library and Drive Configuration window by clicking **Start** and **Exit**. Go to the next step.



If the MediaAgent and CommServe computers are located on opposite sides of a firewall, configure the libraries at a later time using the Library & Drive Configuration window from the CommCell Console after creating the necessary firewall files. For more information on creating these files and configuring Galaxy communications on computers across firewall(s), refer to the *CommServe Administration Guide*.

- 18** For File System clients, click OK if no storage policy exists.



If desired, you can change your storage policy selection at any time after you have installed the File System iDataAgent.

A storage policy directs backup data to a media library. Each library has a default storage policy. When you install the iDataAgent, it creates a default subclient. This subclient can backup the entire NetApp filer.

- 19** Click Finish to close the Setup Complete dialog box.
- 20** A message advises you to create a Job Schedule for the File System in order to secure your data. Click Close to exit the installation.

This task is now complete.

Review the *Post-Install Considerations* on page 1-22, before you begin any operations in the iDataAgent.

Installing the iDataAgent on a Unix Platform

The following steps describe an installation of the NetApp NAS NDMP iDataAgent on the Solaris platform. The Base software and File System iDataAgent must be installed prior to installing the NetApp NAS NDMP iDataAgent. For instructions on installing the Base software and File System iDataAgents, see the *Galaxy Client Installation and Administration Guide (Unix File Systems)*.

❑ To install the iDataAgent on Solaris

Once you have reviewed the *Before You Begin* on page 1-12, you are ready to install the iDataAgent.

If you choose to install multiple components simultaneously, refer to the appropriate *Client Installation and Administration Guide* for installation requirement sand procedures specific to each component. The following procedure describes installing the NetApp NAS NDMP iDataAgent only.

- 1 Log on to the client as `root`.
- 2 Place the software CD-ROM that is appropriate to the computer's operating system into the client's CD-ROM drive.
- 3 Navigate to and execute the `cvpkgadd` command.
- 4 The banner and other information are displayed followed by:

```
This script will install Galaxy 4.2.0 on your machine.
Press ENTER to begin ...
```
- 5 Press `Enter` to review and accept the End User License Agreement.
- 6 Select the module that you want to install. The list displays all of the modules that are not installed.
 - 1) CVGxCM
 - 2) CVGxIDA
 - 3) CVGxProxyIDA
 - 4) CVGxOrIDA
 - 5) CVGxIfIDA
 - 6) CVGxDB2
 - 7) CVGxSAP
 - 8) CVGxSDM
 - 9) CVGxNAS
 - 10) CVGxQuickRecoveryAgent
 - 11) CVGxCXBF
 - 12) Exit

Enter the module number corresponding to the NetApp NAS NDMP iDataAgent (CVGxNAS).

Module number: [9]

7 The following message will display:

We are now ready to copy binaries.

Press ENTER to begin ...

8 A series of messages similar to the following appears. Press Enter to continue.

Updating registry tree under /etc/CommVaultRegistry ... done.

Adding CVGxNAS to /etc/Galaxy.pkg

Successfully installed CVGxNAS.

9 The install program displays the list of modules.

1) CVGxCM

2) CVGxIDA

3) CVGxProxyIDA

4) CVGxOrIDA

5) CVGxIfIDA

6) CVGxDB2

7) CVGxSAP

8) CVGxSDM

9) CVGxQuickRecoveryAgent

10) CVGxCXBF

11) Exit

Enter the appropriate value to exit the install program.

Module number: [11]

This task is now complete.

Installing the NDMP Remote Server (NRS) on a Unix MediaAgent

If your Unix MediaAgent has a library attached and is used by a NetApp NAS NDMP iDataAgent to backup data, you must install the NRS software. The following steps describe an installation of the NRS software on the Solaris platform.

To install NRS on a Unix MediaAgent

Once you have reviewed *Before You Begin* on page 1-12, you are ready to install NRS on a UNIX filer.

If you choose to install multiple components simultaneously, refer to the appropriate *Client Installation and Administration Guide* for installation requirements and procedures specific to each component. The following procedure describes installing the NRS iDataAgent only.

- 1 Log on to the MediaAgent as `root`.
- 2 Place the software CD-ROM that is appropriate to the computer's operating system into the client's CD-ROM drive.
- 3 Select the module that you want to install. The list displays all of the modules that are not installed.
 - 1) CVGxCM
 - 2) CVGxIDA
 - 3) CVGxProxyIDA
 - 4) CVGxOrIDA
 - 5) CVGxIfIDA
 - 6) CVGxDB2
 - 7) CVGxSAP
 - 8) CVGxSDM
 - 9) CVGxNAS
 - 10) CVGxNRS
 - 11) CVGxQuickRecoveryAgent
 - 12) CVGxCXBF
 - 13) Exit

Enter the module number corresponding to the NetApp NAS NDMP Remote Server (CVGxNRS).

Module number: [10]

4 The following message will display:

We are now ready to copy binaries.

Press ENTER to begin ...

5 You will be prompted for the account name and password.

Would you like to provide NDMP Remote Server Account Name and Password now?

Note that it will be possible to add/modify the Account information later using the NAS Client Wizard Tool.

Add Account Name and Password? [yes]

Press Enter.

6 You will be prompted for your account name:

Please enter NDMP Remote Server Account Name.

Account Name:

Type account name this is for galaxy's internal use, better to write down this account and password for future use

Input the account name and press Enter.

7 You will be prompted you for your password.

Please enter NDMP Remote Server Account Password.

Password:

Again:

Input the password twice and press Enter.

8 The install program completes the installation.

Sending account information to the CommServe ... done.

Creating CVNdmpRemoteServer service ... done.

Starting Galaxy services ... done.

Adding CVGxNRS to /etc/Galaxy.pkg

Successfully installed CVGxNRS.

Press ENTER to continue ...

The install program displays the list of modules.

- 1) CVGxCM
- 2) CVGxIDA
- 3) CVGxProxyIDA
- 4) CVGxOrIDA
- 5) CVGxIfIDA
- 6) CVGxDB2
- 7) CVGxSAP
- 8) CVGxSDM
- 9) CVGxNAS
- 10) CVGxQuickRecoveryAgent
- 11) CVGxCXBF
- 12) Exit

Enter the appropriate value to exit the install program.

Module number: [12]

This task is now complete.

Review the *Post-Install Considerations* on page 1-22, before you begin any operations in the iDataAgent.

Post-Install Considerations

If you have not configured the library and drives, you must do so now. For more information, see *Configuring Libraries and Drives for NetApp NAS NDMP iDataAgent* on page 1-23.

If you have already configured the library and drives, you must now add the NetApp NAS NDMP clients. For more information, see *Adding Clients for NetApp NAS NDMP iDataAgents* on page 1-51.

Configuring Libraries and Drives for NetApp NAS NDMP iDataAgent

NetApp NAS NDMP iDataAgent differs from other iDataAgents in that the data can either be:

- ◆ Backed up to a library attached to the filer, without the data passing through a MediaAgent.
- ◆ Backed up to a library attached to the MediaAgent only when NDMP Remote Server installed.
- ◆ Backed up to a library attached to a SAN network.

In all these cases, the iDataAgent uses the NDMP protocol to communicate with the filer.

Configuring the Library and Drives Attached to a NetApp filer

We recommend that you configure the library and drives attached to a NetApp filer using the automatic detection procedure described in *To configure a library and drives attached to the NetApp filer using automatic detection* on page 1-24.

If the automatic detection process fails use the manual detection process described in *To manually configure the library and drives attached to the NetApp filer* on page 1-31

Refer to the NetApp filer documentation for the following:

- ◆ Information on attaching the hardware to the filer.
- ◆ Information on the library and drive types supported by your NetApp filer.

Before You Begin

Review the following to avoid common problems:

- ◆ Verify that the NDMP service is enabled on the filer. This is not enabled by default.
For information on enabling NDMP service, see *Appendix F, Enabling NDMP Service*
- ◆ Verify that the tape drive and media changer, if attached to the NetApp filer, is detected by the filer.
For information on verifying tape drive(s) and media changer, see *Appendix D, Obtaining Information from the NetApp Filer*.

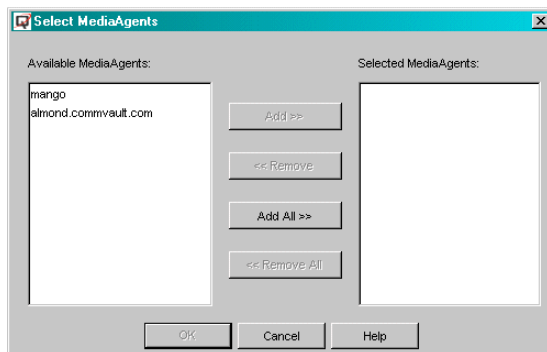
You can add and configure NDMP drives after installing the MediaAgent.

This section contains the following procedures:

- ♦ *To configure a library and drives attached to the NetApp filer using automatic detection on page 1-24*
- ♦ *To manually configure the library and drives attached to the NetApp filer on page 1-31*

□ To configure a library and drives attached to the NetApp filer using automatic detection

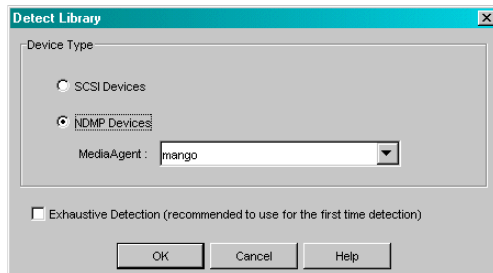
- 1 After installation, from the CommCell Console, select Tools -> Library & Drive Configuration.



- 2 In the Select MediaAgents dialog box, highlight the MediaAgent on which the library attached to the NetApp filer is to be configured, click Add and click OK.

If a device has already been configured for the MediaAgent, the system displays the devices in the Galaxy Library and Drive Configuration window.

- 3 From the Galaxy Library and Drive Configuration window, click the Start button, and then select Detect/Configure Devices.



- 4 In the Detect/Configure Devices dialog box, choose NDMP Devices and then select the MediaAgent that will control the library.
- 5 Select NDMP Devices and Exhaustive Detection option, and click OK.

The exhaustive detection process accurately maps the drives in a library. During this process, the system attempts to mount a tape in each of the selected drives and determines the correct drive to library mapping. Due to the nature of this operation and depending on the number of drives, this operation may take several minutes to complete.



As this operation involves the mounting of a tape in a drive, ensure that there are some media in the library to mount. If you do not select Exhaustive Detection, the system still attempts to discover the media changer and drives connected to the selected NDMP host, but the system will not mount tapes in those drives to confirm the correct drive mapping.

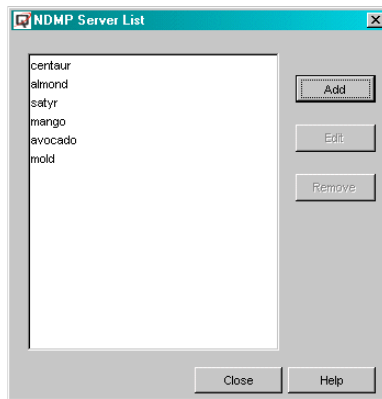
- 6 A prompt appears informing you that the exhaustive detection will unload all drives and hence may interfere with backup/restore jobs. Click Yes to continue.

- 7 From the Galaxy Library and Drive Configuration window, click the Start button, point to NDMP, and then select Servers from the short-cut menu.

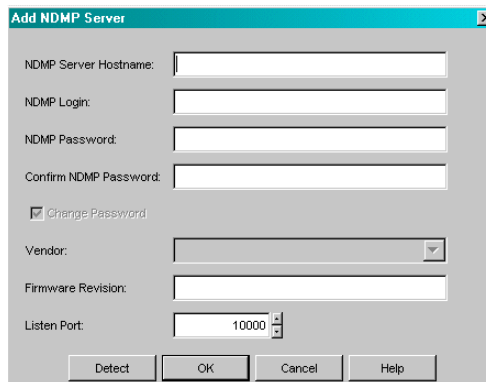
Or

From any dialog box that contains an Update NDMP Server List button, click this button.

The following NDMP Server List dialog box is displayed.

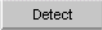


- 8 Select an NDMP Server and click the Add button.



- 9 In the Add NDMP Server dialog box, enter the following information:

NDMP Server	The long name of the NetApp filer.
Hostname	

NDMP Login	The user account through which the system will access the filer. For NetApp, this account must be <code>root</code> .
NDMP Password	The password for the NDMP Server Login account.
Confirm NDMP Password	The password for the NDMP Server Login account, for confirmation.
	When clicked, the system automatically populates the Vendor, Hardware OS Revision and Listen Port information.



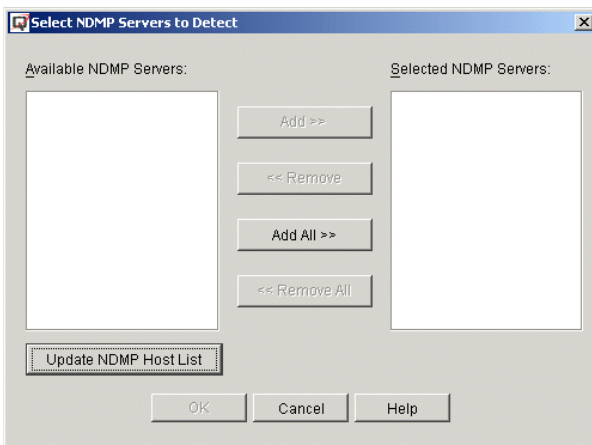
NOTE

If the NetApp filer version does not support detection, the user will have to enter the Vendor and Firmware Revision information manually.

When you are finished, the information in this dialog box should be similar to the following image.

- 10 Click OK.
- 11 The system displays the NDMP Server List dialog box. Click Close to complete the process or go to step 8 to select another server.

- 12** In the Detect Devices Options dialog box, select the NDMP Host(s) (NetApp filer) to which the library(s) you would like to detect are attached. Click Add>> to select a single server or click Add All>> to select all the servers listed.

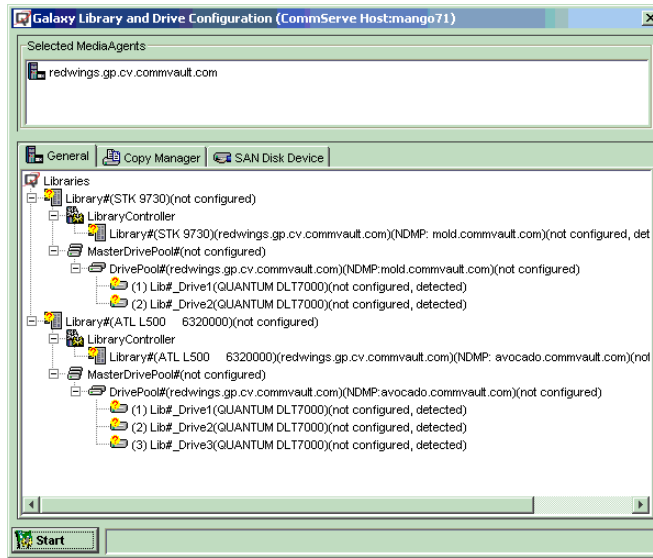


- 13** Click OK.

A prompt appears informing you that the Library Management Services (LMS) will be stopped and restarted. Click Yes to start the device detection process.

The system attempts to detect the devices and mount the media in the drives to verify the correct drive to library mapping.

When the exhaustive detection is completed, the system displays the devices in the Galaxy Library and Drive Configuration window.

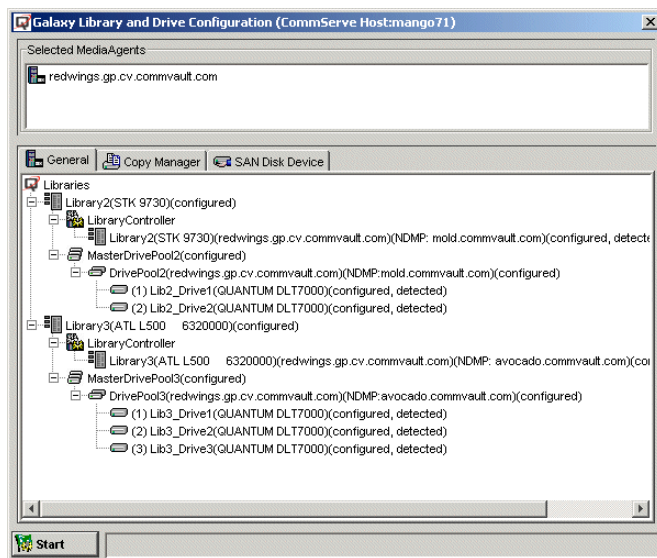


NOTE

Note that new detected devices are not configured at this point, and the configuration information will not be saved when you exit from the Galaxy Library and Drive Configuration window until those devices are configured.

- 14 Configure the library. To configure, right-click the library and then click **Configure**.
- 15 A Configuration dialog box appears, asking if you would like to configure the library or the library and the drives.
 - If you want to configure all of the drives within the library, select **Library and all drives** and click **OK**.
 - If you want to configure the drives individually, select **Library Only**. Click **OK**.
- 16 A prompt box appears asking if this library has a bar code reader. Click **Yes** or **No**.

- 17 A prompt appears asking if you want to automatically detect the media. Click Yes or No.
- 18 If you have configured the library, the status of the library changes to **configured**. If you chose to configure all associated drives, the status of the drives (and the master drive pool and drive pool that contains the drives) changes to **configured** as well.



The task is now complete.

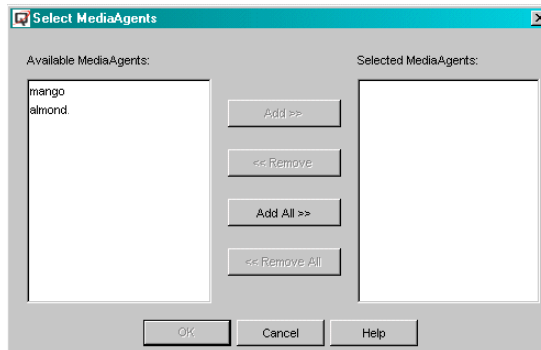
You must now add the NetApp NAS NDMP clients. For more information, see *Adding Clients for NetApp NAS NDMP iDataAgents* on page 1-51.

- ❑ To manually configure the library and drives attached to the NetApp filer



You should not manually configure a library unless automatic detection of the library failed.



- 1 At the CommCell Console, select Tools -> Library and Drive Configuration.



- 2 In the Select MediaAgent dialog box, highlight the MediaAgent, on which the library attached to the NetApp filer is to be configured, click Add and click OK.
If a device has already been configured for the MediaAgent, the system displays the devices in the Galaxy Library and Drive Configuration window.
- 3 From the Galaxy Library and Drive Configuration window, click the Start button, point to NDMP and then Add Library from the short-cut menu.

- 4 The following Add Library dialog box is displayed.

- 5 In the Add NDMP Library dialog box, enter the following information:

MediaAgent	The name of the MediaAgent that will control the library attached to the filer.
NDMP Server Hostname	The name of the NetApp filer. Keep in mind that you must add at least one host before selecting a host from this field.
	Opens the NDMP Server List dialog box which allows you to add or edit existing hosts.
NDMP Server Device Name	The access path through which the filer communicates with the media changer in the library. A typical value for the first device (media changer) is mc0. For more information on server device names, see <i>Obtaining the Device Name of Media Changer</i> on page D-2.
	When clicked, the system automatically populates the Library Data which includes the Vendor, Model, Firmware, Base Address and Drive Count.

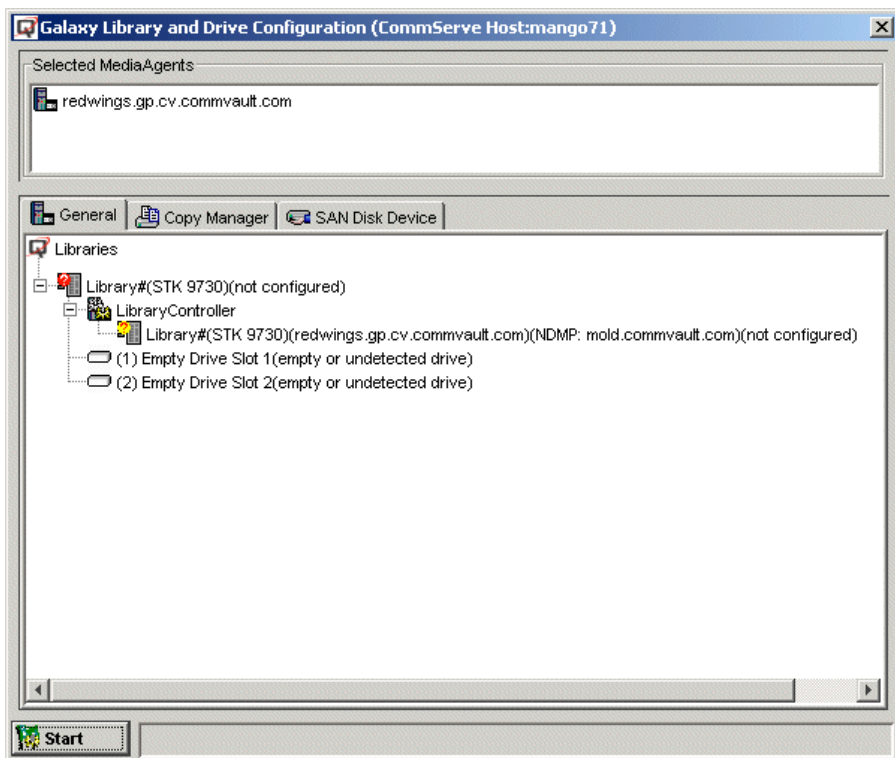


If the library is not supported by the NetApp device, an error message is displayed when you click the **Detect Library Data** button. Contact your CommVault Systems representative for assistance.

The information in this dialog box should be similar to the following image.

- 6 When you are finished, click OK.

The Galaxy Library and Drive Configuration window displays the library information, with the not configured status, and place holders for the drives in the library, as shown in the following image.




Adding the Drives

- 7 From the Galaxy Library and Drive Configuration window, click the Start button, point to NDMP, and then select Add Drive from the short-cut menu.

8 The following Add NDMP Drive dialog box, is displayed.

9 In the Add NDMP Drive dialog box, enter the following information:

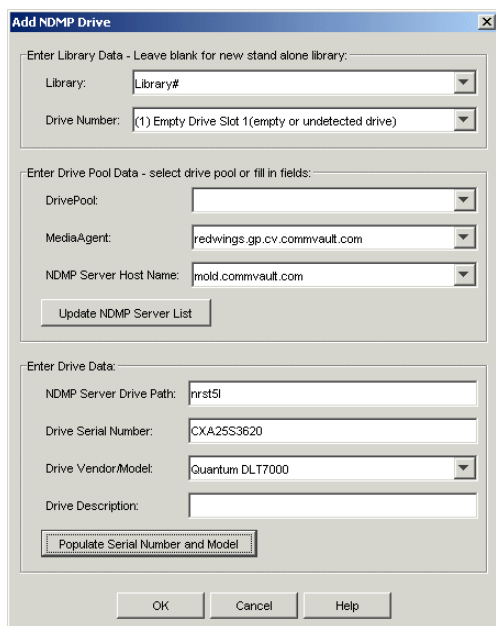
Library	The name of the library containing the drive.
Drive Number	The physical location of the drive.
DrivePool	If you are adding the first drive for the library, leave the field blank. If a drive pool has already been created for this filer, select the name of the drive pool from the list.
MediaAgent	The name of the MediaAgent that controls the library’s media changer.
NDMP Server Host Name	Select the name of the filer from the drop-down menu. Keep in mind that you must add the host to which the library is connected before selecting the host from this field. Click on the Update NDMP Server List button to add a host.

 Opens the NDMP Server List dialog box which allows you to add or edit existing hosts.

NDMP Server Drive Path The access path through which the filer communicates with the drive. For additional information, see *Obtaining the Device Name of Media Changer* on page D-2.

- 10 Click the **Populate Serial Number and Model** button. This automatically populates the **Drive Serial Number** and **Drive Vendor/Model** fields. If this does not work automatically, you have to add the information manually.
- 11 Type a text description of the drive (e.g., NetApp filer ADIC drive 1) in the **Drive Description** field. (Optional).

The information in this dialog box should be similar to the following image.



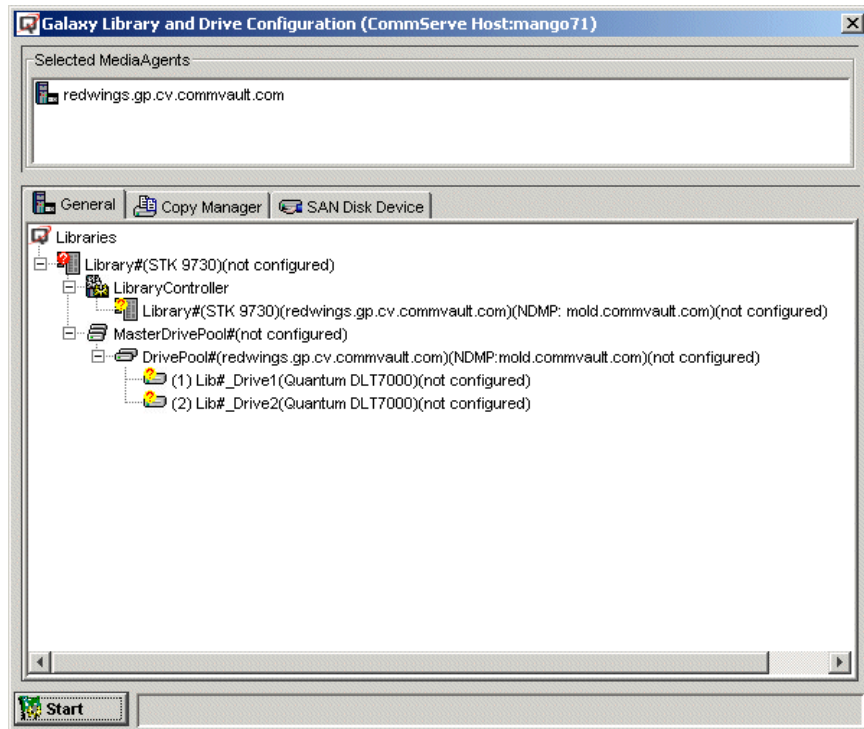
The image shows a Windows-style dialog box titled "Add NDMP Drive". It is divided into three main sections:

- Enter Library Data - Leave blank for new stand alone library:**
 - Library:** A dropdown menu with "Library#" selected.
 - Drive Number:** A dropdown menu with "(1) Empty Drive Slot 1 (empty or undetected drive)" selected.
- Enter Drive Pool Data - select drive pool or fill in fields:**
 - DrivePool:** A dropdown menu.
 - MediaAgent:** A text field containing "redwings.jp.cv.commvault.com".
 - NDMP Server Host Name:** A text field containing "mold.commvault.com".
 - Update NDMP Server List** button.
- Enter Drive Data:**
 - NDMP Server Drive Path:** A text field containing "hrrst5l".
 - Drive Serial Number:** A text field containing "CXA25S3620".
 - Drive Vendor/Model:** A dropdown menu with "Quantum DLT7000" selected.
 - Drive Description:** An empty text field.
 - Populate Serial Number and Model** button.

At the bottom of the dialog are three buttons: **OK**, **Cancel**, and **Help**.

- 12 When you are finished, click **OK**.

The Galaxy Library and Drive Configuration window displays the drive information, with the not configured status, as shown in the following image.

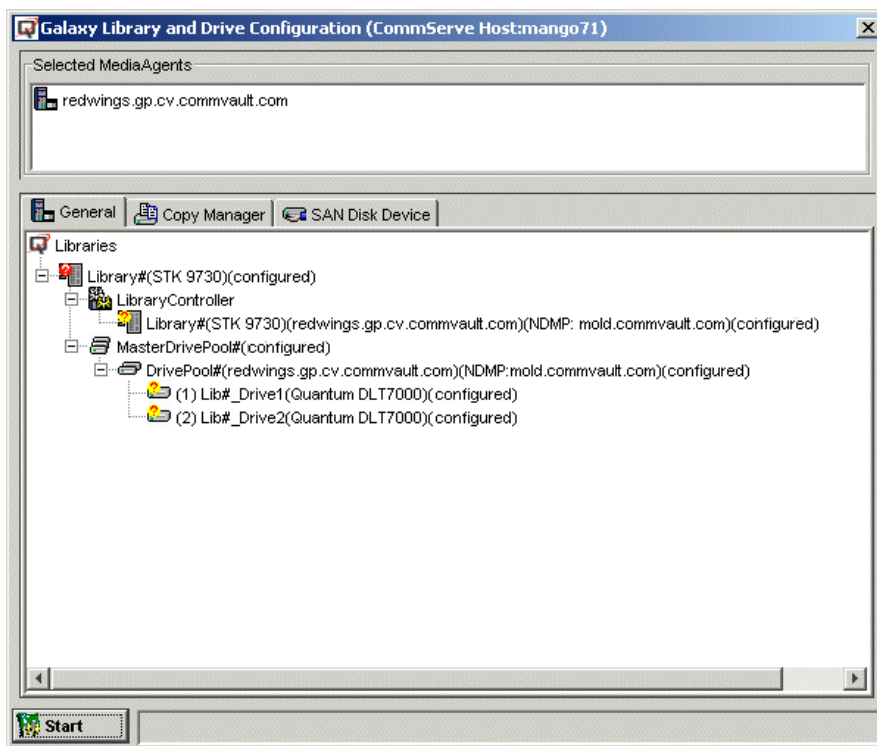


Note that if the devices are not configured at this point, the configuration information will not be saved when you exit from the Galaxy Library and Drive Configuration window.

Repeat this process until all drives are configured.

- 13** After all of the drives attached to the filer have been added, configure the library. To configure, right-click the library and then click *Configure*.

- 14 A Configuration prompt appears, asking if you would like to configure the library or the library and the drives.
 - If you want to configure all of the drives within the library, select `Library and all drives` and click OK.
 - If you want to configure the drives individually, select `Library Only`.
Click OK.
- 15 The Device Configuration dialog box appears. Select either `Do Exhaustive Detection Now` or `Configure Devices without Exhaustive Detection`. Click OK.
- 16 A prompt box appears asking if this library has a bar code reader. Click `Yes` or `No`.
- 17 If you have configured the library, the status of the library changes to `configured`. If you chose to configure all associated drives, the status of the drives (and the master drive pool and drive pool that contains the drives) changes to `configured` as well.



- 18 At the prompt to select media type, select the media type and select whether you want to auto-discover media. If you select **No**, you will have to discover media for the library manually later.
- 19 If you did not choose exhaustive detection, we recommend that you validate the library after it is configured to ensure that the library is accessible to the system. To validate the library, right-click the library and then click **Validate**. Click **Yes** in the prompt informing you that the validation may take several minutes.

The system attempts to mount a media in each drive within the library. A status message reporting the success or failure of the operation appears in the Status Bar of the **Galaxy Library and Drive Configuration** window.

The task is now complete.

You must now add the NetApp NAS NDMP clients. For more information, see *Adding Clients for NetApp NAS NDMP iDataAgents* on page 1-51.

Configuring Stand-alone Drives attached to a NetApp filer

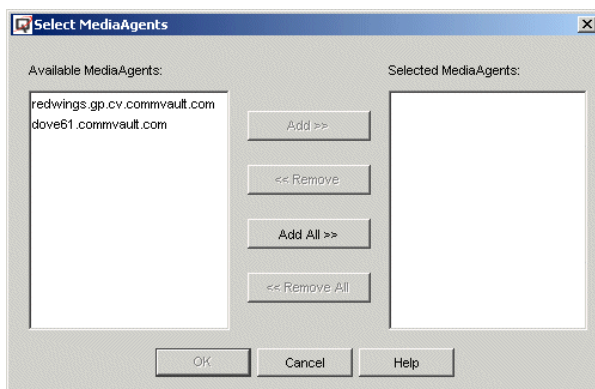
You can share the drives from a library attached to the NetApp filer to other MediaAgents, by configuring them as a stand-alone drive on these MediaAgents. This may be necessary when you need to use a library attached to the NetApp filer to backup other resources.

The following procedure outlines the steps involved in configuring a drive as a stand-alone drive. Note that this operation has to be performed on the MediaAgent in which you wish to configure the drive.

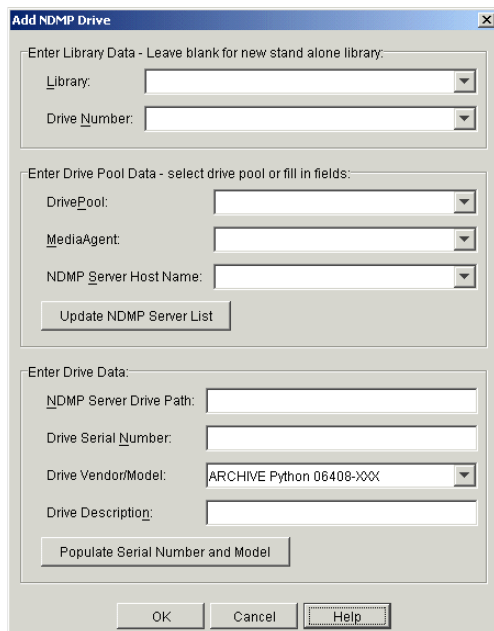
☐ To configure a stand-alone drive on a library attached to the NetApp filer

- 1 At the CommCell Console, select **Tools -> Library and Drive Configuration**.

- 2 In the Select MediaAgent dialog box, highlight the MediaAgent on which the library attached to the NetApp filer is to be configured, click Add and click OK.



- 3 From the Galaxy Library and Drive Configuration window, click the Start button, point to NDMP, and then select Add Drive from the short-cut menu.
- 4 The following Add NDMP Drive dialog box, is displayed.



- 5 In the Add NDMP Drive dialog box, enter the following information:

Library Leave this field blank.

Drive Number Leave this field blank.

DrivePool Leave this field blank.

If a value exists in this field, be sure to remove it before continuing.

MediaAgent The name of the MediaAgent controlling the drive.

NDMP Server
Host Name Select the name of the filer from the drop-down menu. Keep in mind that you must add at least one host before selecting the host from this field. Click on the Update NDMP Server List button to add a host.



Opens the NDMP Server List dialog box which allows you to add or edit existing hosts.

NDMP Server
Drive Path The access path through which the filer communicates with the drive. For additional information, see *Obtaining the Drive Access Path* on page D-3.

- 6 Click the Populate Serial Number and Model button. This automatically populates the Drive Serial Number and Drive Vendor / Model fields. If this does not work automatically, you have to add the information manually.
- 7 Type a text description of the drive (e.g., NetApp filer ADIC drive 1) in the Drive Description field. (Optional).

The information in this dialog box should be similar to the following image.

Add NDMP Drive

Enter Library Data - Leave blank for new stand alone library:

Library:

Drive Number:

Enter Drive Pool Data - select drive pool or fill in fields:

DrivePool:

MediaAgent:

NDMP Server Host Name:

Enter Drive Data:

NDMP Server Drive Path:

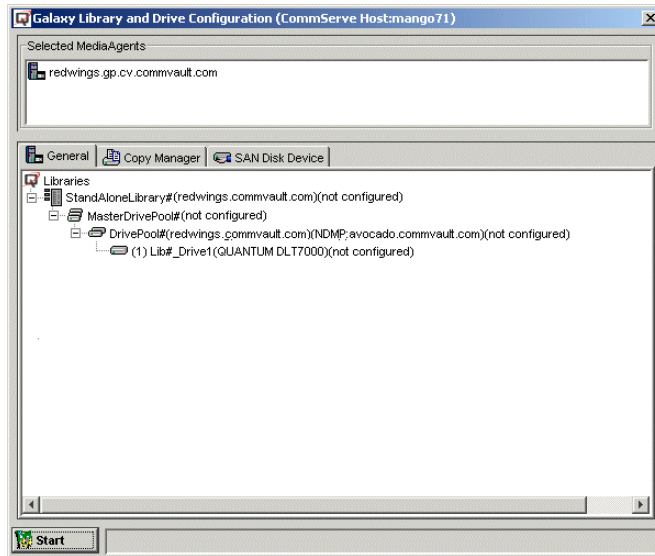
Drive Serial Number:

Drive Vendor/Model:

Drive Description:

8 When you are finished, click OK.

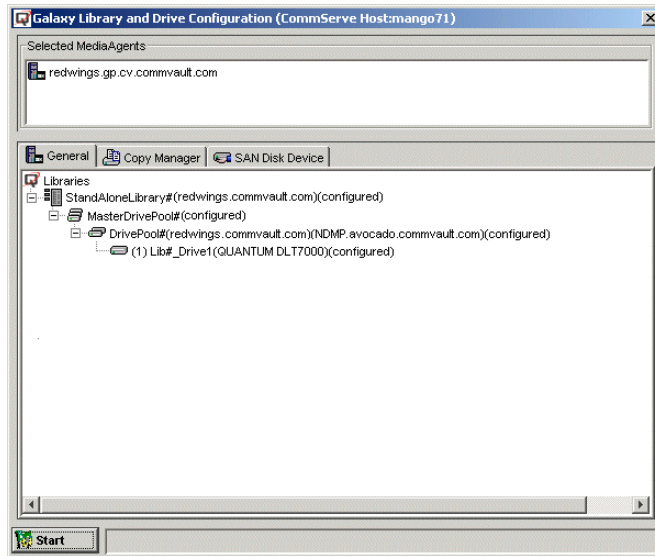
The system creates a standalone library tree for the drive in the Galaxy Library and Drive Configuration window, as shown in the following image.



Note that if the drive is not configured at this point, the configuration information will not be saved when you exit from the Galaxy Library and Drive Configuration window.

- 9 Configure the drive. To configure, right-click the stand-alone library and then click Configure.

- 10 After the configuration, the status of the drive, drive pool, master drive pool and stand-alone library changes to configured.



The task is now complete.

You must now add the NetApp NAS NDMP clients. For more information, see *Adding Clients for NetApp NAS NDMP iDataAgents* on page 1-51.

Configuring a Library Attached to a MediaAgent and used by the NetApp NAS NDMP iDataAgent

Before You Begin

Review the following to avoid common problems:

- ♦ Install MediaAgent on the computer that is used as MediaAgent by the NetApp NAS NDMP iDataAgent.
- ♦ During the MediaAgent installation, in the `MediaAgent Install Options` you must have selected the `Media Agent With NDMP Remote Server` option.
- ♦ Verify this MediaAgent host name is in the NDMP Host List.
- ♦ If the library is attached to a Solaris MediaAgent, refer to *Installing the iDataAgent on a Unix Platform* on page 1-16 for instructions on installing the NDMP Remote Server on a Solaris MediaAgent.

Follow the procedure for configuring libraries and drives as described in the *CommCell Media Management Administration Guide*, under the section *Library Configuration Procedures*.

Dynamic Drive Sharing (DDS) Between Multiple Devices in a SAN Environment

The drives in a library can be dynamically shared (DDS) between multiple devices, (NetApp filers and MediaAgents) if these devices are connected to the library in a SAN environment. In a SAN environment, the primary consideration would be the device controlling the media changer, which is the first configured device. For example, if you share a library between two filers the first filer will control the media changer. The same rule applies for a library shared between a MediaAgent(s) and filer(s).

Before You Begin

Review the following to avoid common problems:

- ◆ During configuration, all of the drive devices must have a value for their serial number. If the configuration wizard does not populate a serial number for a drive, you must manually enter a serial number value. Each instance of a drive must have the same serial number.

❑ To dynamically share drives between multiple devices in a SAN environment

The following procedure explains the steps involved in configuring a library which is shared in the SAN environment between two NetApp filers.

Configuring the first device

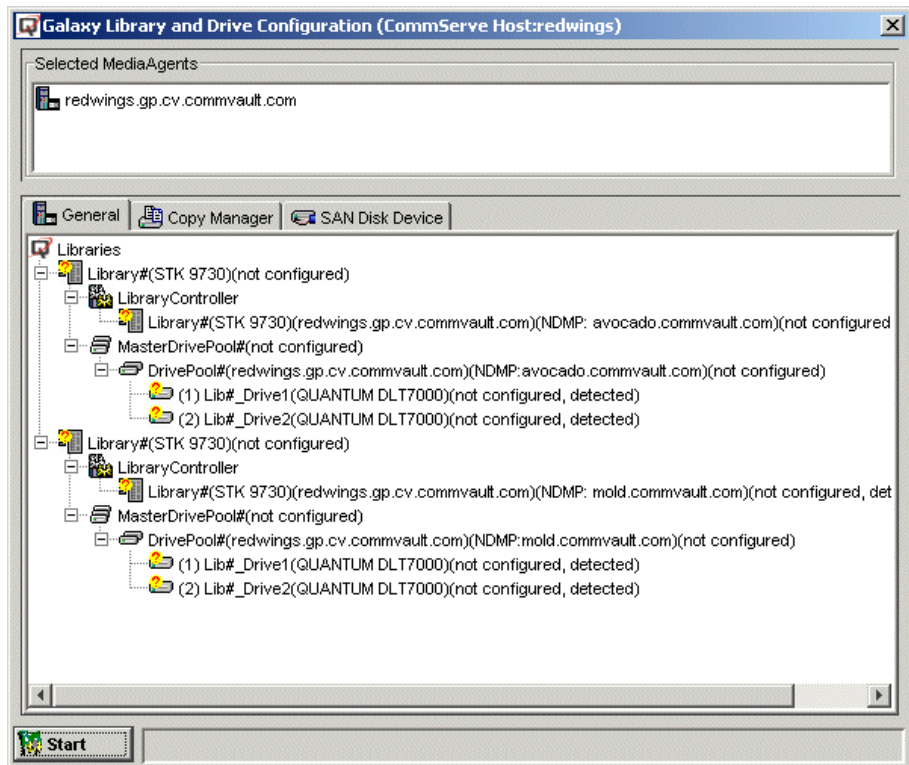
- 1 Follow the procedure *To configure a library and drives attached to the NetApp filer using automatic detection* on page 1-24. Perform Steps 1-13.



NOTE

When you get to Step 12, in the Detect Devices Options dialog box, select **all** NDMP servers and Media Agents that will dynamically share the library. (The library must be connected to each of the selected NDMP servers through a fibre channel switch.)

At this point, the Galaxy Library and Drive Configuration window should be similar to the following image.



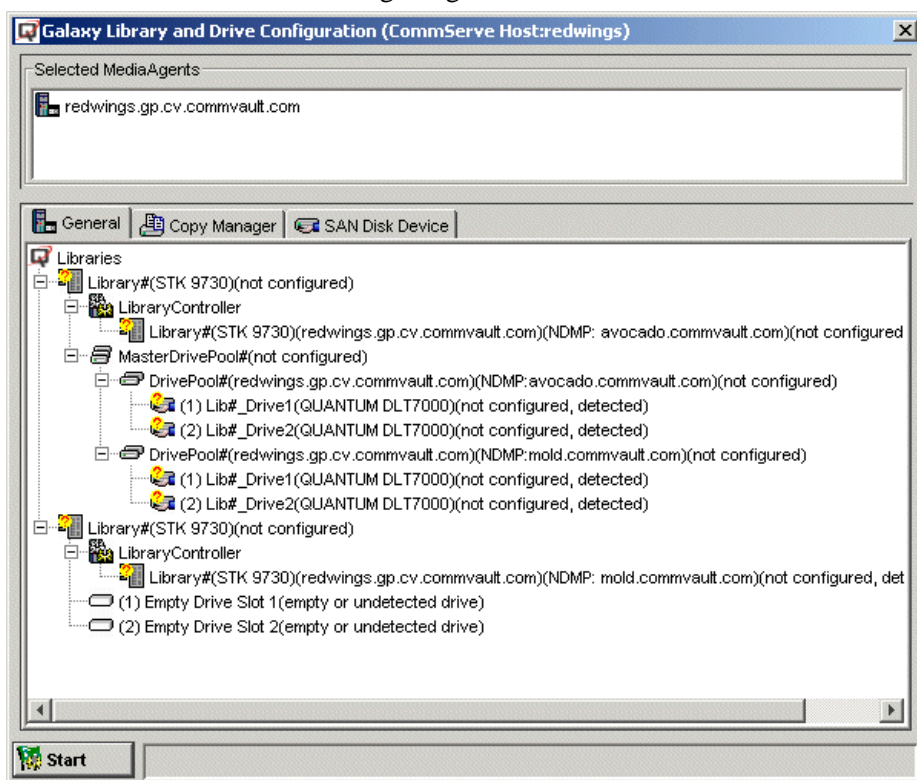
Create a DDS Drive Pool

- 2 Drag and drop a detected Drive Pool from one instantiation of the library for one of the NDMP servers, onto the Master Drive Pool of another instantiation of the library for a different NDMP server.

You will be prompted about creating a SAN Drive Pool.

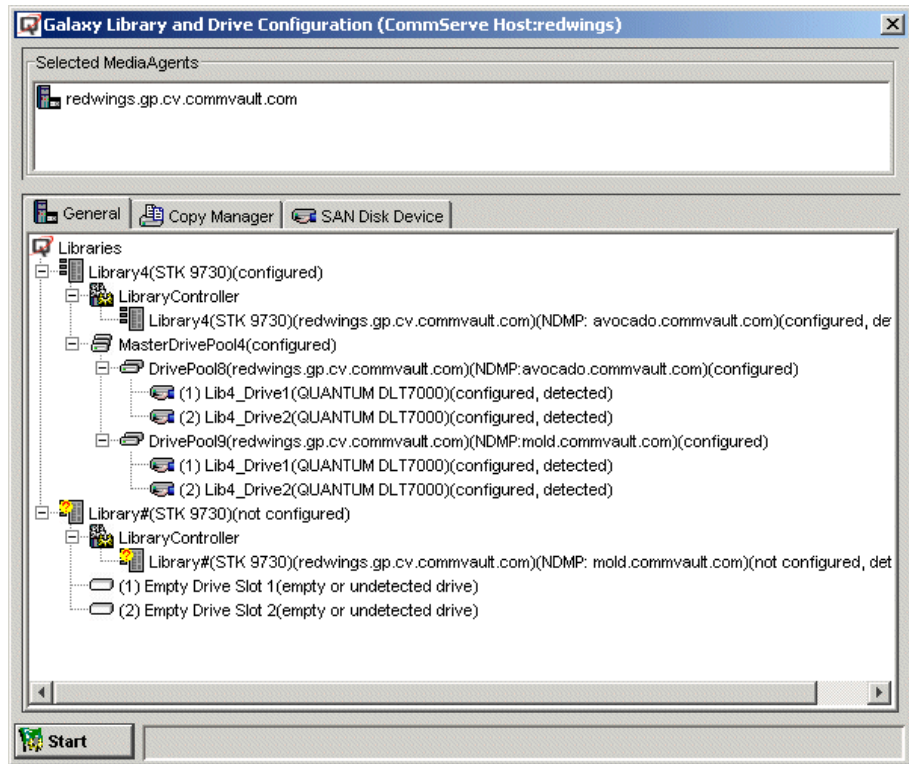
Click Yes to continue.

At this point, the Galaxy Library and Drive Configuration window should be similar to the following image.



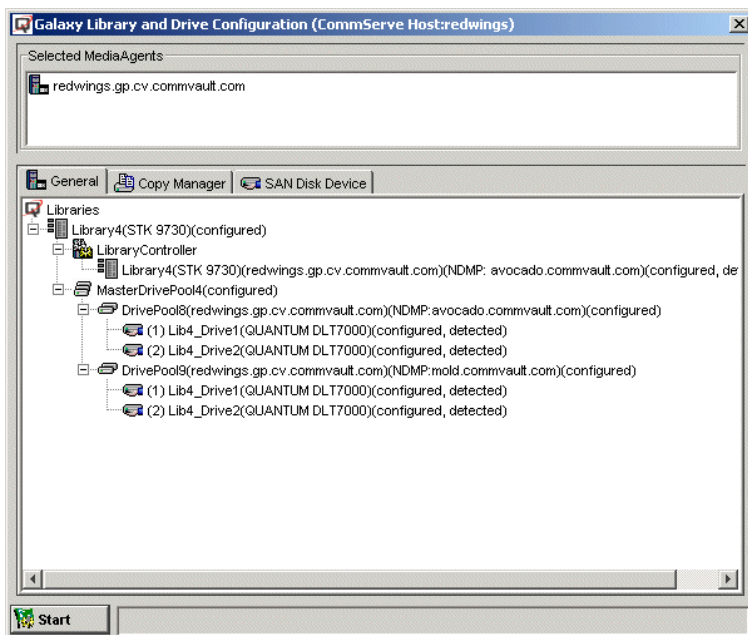
- 3 Repeat Step 2 for all NDMP servers or MediaAgents that will dynamically share this library.

- 4 To configure the library, right-click the library and then click Configure.



- 5 A Configuration dialog box appears, asking if you would like to configure the library or the library and the drives.
 - ◆ If you want to configure all of the drives within the library, select **Library and all drives** and click OK.
 - ◆ If you want to configure the drives individually, select **Library Only**.
 - ◆ Click OK.
- 6 A prompt box appears asking if this library has a bar code reader. Click Yes or No.
- 7 A prompt appears asking if you want to automatically detect the media. Click Yes or No.

- 8 After the configuration the status of the drive and drive pool changes to configured.



- 9 If you do not need to configure any other libraries, exit now.



If there are additional unconfigured libraries shown that you do not need, you can delete them.

This task is now complete.

You must now add the NetApp NAS NDMP clients. For more information, see *Adding Clients for NetApp NAS NDMP iDataAgents* on page 1-51.

Adding Clients for NetApp NAS NDMP iDataAgents

The following procedure describes the steps for adding the NetApp clients to the CommCell.

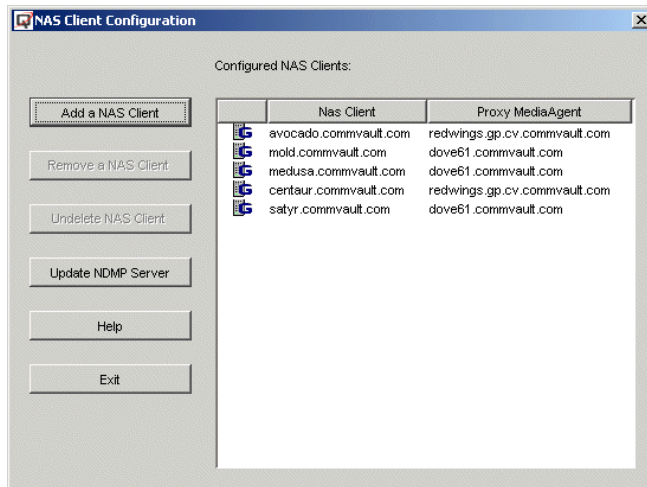
Before You Begin

Review the following to avoid common problems:

- ◆ You have an available license on the CommServe for the NetApp NAS NDMP client you wish to add.

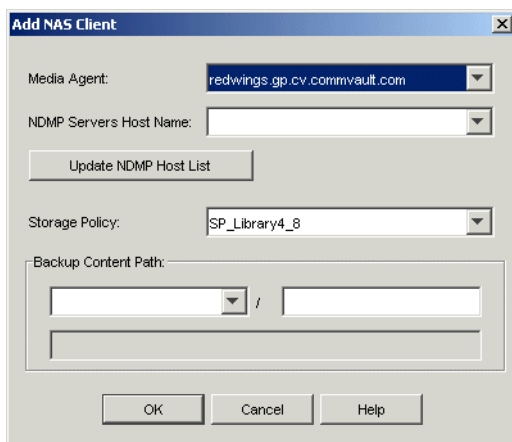
❑ To add a NAS client

- 1 From the CommCell Console, select **Tools** and **NAS Client Configuration**.



- 2 From this window, you can add any filer on the network. Click **Add a NAS Client**.

- 3 The following Add NAS Client dialog box appears.



The image shows a Windows-style dialog box titled "Add NAS Client". It contains several fields and buttons. At the top, there is a dropdown menu for "Media Agent:" with the value "redwings.gp.cv.commvault.com". Below it is a dropdown menu for "NDMP Servers Host Name:". A button labeled "Update NDMP Host List" is positioned below the "NDMP Servers Host Name:" dropdown. Further down is a dropdown menu for "Storage Policy:" with the value "SP_Library4_8". Below that is a section for "Backup Content Path:" which includes a dropdown menu, a slash "/", and a text input field. At the bottom of the dialog are three buttons: "OK", "Cancel", and "Help".

- 4 Select and/or enter the following information:

MediaAgent	The name of the computer hosting the MediaAgent on which you are currently installing the NetApp NAS NDMP iDataAgent.
NDMP Servers Host Name	The name of the NetApp filer that is selected from a drop-down menu.
Update NDMP Host List	Allows you to add or edit existing hosts to the NDMP host list.
Storage Policy	The name of the storage policy for NAS data and index. This is the storage policy that was created when you configured the drive pool for the NDMP drive.
Backup Content Path	The path for the backup content of the default subclient.



Because NetApp filers define their directories as different portions of a specific root directory on a file server or storage processor, the subclient must contain the full path of the content you want to back up, including the correct root directory. Once your CommCell console is fully configured, you will be given the opportunity to add additional paths to the default subclient, or create additional subclients, which you can define for each directory. At that time, refer to the help provided with the software for more information on subclient definition and for steps involved in changing the content of the subclient.

- 5 Click OK.
- 6 After all of the NetApp NAS NDMP iDataAgents are configured, click **Exit** in the **NAS Client Configuration** window.

The task is now complete.

System Overview

This chapter describes the CommVault® QiNetix™ software architecture and specific features in the NetApp NAS NDMP iDataAgent/agent that can be used to manage data.

This chapter contains:

- ◆ Introduction, 2-2
- ◆ What You Need to Know About the NetApp NAS NDMP iDataAgent, 2-7
- ◆ What You Need to Know About Galaxy, 2-8
- ◆ Subclients, 2-9
- ◆ NDMP Remote Server, 2-12
- ◆ Storage Policies, 2-13
- ◆ Backup Sets, 2-27

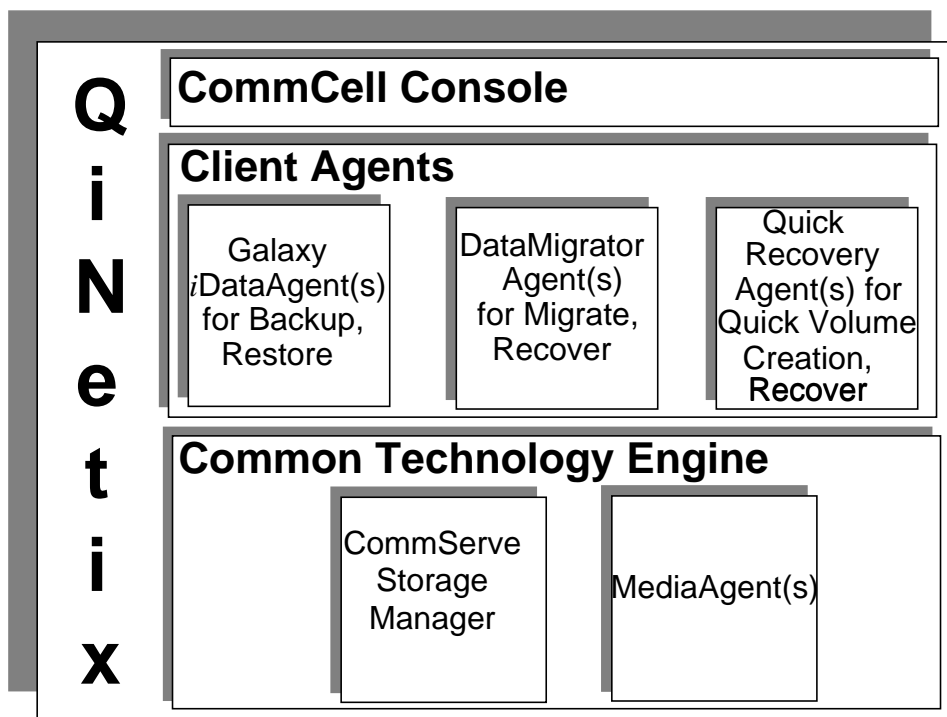
Introduction

CommVault QiNetix software provides a powerful set of storage management tools that help you move and manage your critical data. These tools enable you to store and retrieve data associated with computer systems in your enterprise.

The QiNetix software consists of integrated software modules which can be grouped together in a CommCell™. Each CommCell consists of the following main components:

- ◆ One or more of the following Client Agents:
 - iDataAgents™ that perform the backup and restore operations
 - DataMigrator™ agents that perform the data migration, archival and recovery operations
 - Quick Recovery (QR) agents that create and recover QR volumes
- ◆ The Common Technology Engine (CTE) components consisting of:
 - One CommServe StorageManager™
 - One or more MediaAgents™

Once installed and configured, these CommCell elements can be controlled and monitored from a single unified CommCell Console™.



Client Agents

Client Agents are software modules that perform data protection and data recovery operations for specific operating systems or applications. Multiple agents may be used to protect all types of data residing on a computer. The following sections provide a brief description of each of these Client Agents.

iDataAgents

iDataAgents are software modules that are used for backing up and restoring data. QiNetix software provides a variety of iDataAgents, each one designed to handle a different kind of data. If a given computer has two or more types of data, it requires one iDataAgent for each data type. For example, to secure all the data on a computer where a Microsoft Exchange Server resides, you would need the following iDataAgents:

- ♦ One Windows File System iDataAgent to back up the computer's file system.
- ♦ One Microsoft Exchange Database iDataAgent to back up the database.

In the CommCell Console, such a configuration would appear as two *iDataAgents* on a client computer.

DataMigrator Agents

DataMigrator Agents are software modules that are responsible for periodically moving unused or infrequently used data on their host computers to secondary storage, thereby reducing the size of data on the primary storage. QiNetix software provides several DataMigrator Agents, each one designed to handle a different kind of data. DataMigrator Agents reduce the duration of backup windows by reducing the amount of data to be backed up by an *iDataAgent*.

Quick Recovery Agents

Quick Recovery agents are software modules that use the snapshot technology to create Quick Recovery (QR) volumes on magnetic disks. These QR volumes can be easily recovered in minutes. Quick Recovery Agent integrates with major storage-intensive applications, such as Microsoft SQL Server 2000, Microsoft Exchange 2000 and Oracle, to ensure that data objects are properly synchronized and easily recovered. Quick Recovery Agents augment the traditional backup and restore operations of an *iDataAgent* by allowing the user to create frequent images of the data which provides faster application recovery, when needed; while *iDataAgents* can be used to perform the traditional backup and restore operations of these images.

Common Technology Engine

Common Technology Engine consists of software modules that provide the necessary tools to manage and administer the Client Agents and also manage the storage media associated with the CommCell. The following sections describe the components of the Common Technology Engine.

CommServe StorageManager

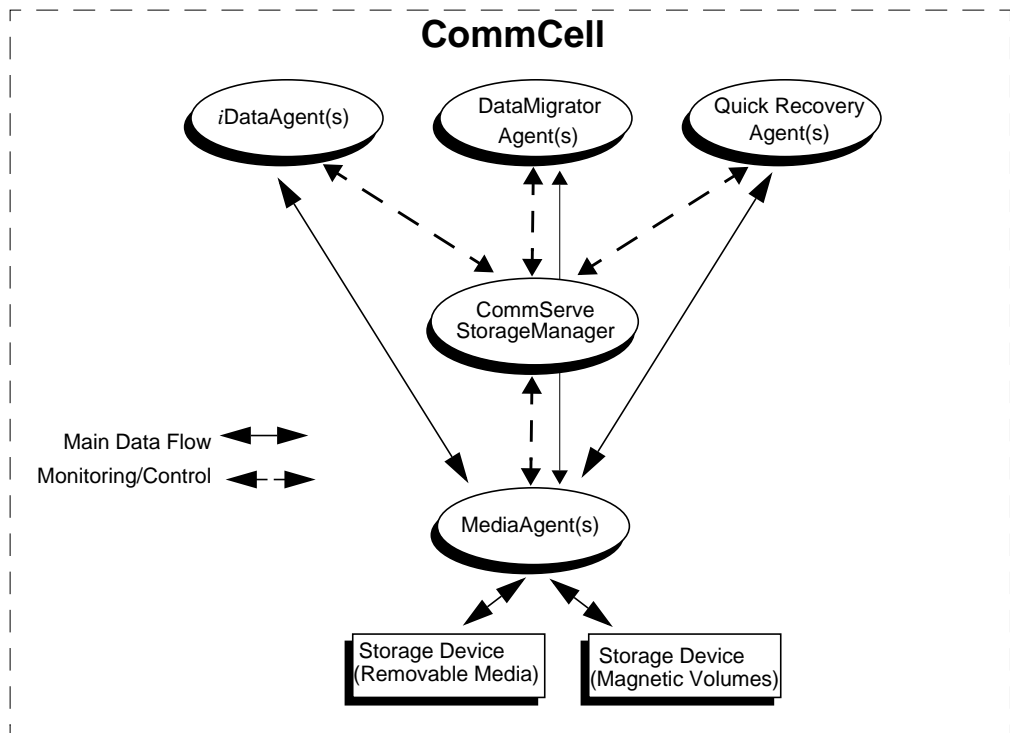
The CommServe™ ties the elements of the CommCell together; it is the coordinator and administrator of the CommCell. The CommServe communicates with all agents in the CommCell to initiate data protection, management and recovery operations. Similarly, it communicates with MediaAgents when the media subsystem requires management. The CommServe maintains a database containing all the information relating to the CommCell. In addition, it provides several tools to administer and manage the CommCell.

MediaAgents

The MediaAgent transfers data between the client computer(s) and the storage media. Each MediaAgent communicates locally or remotely to one or more storage devices, which contains the storage media. The QiNetix system provides support for a wide variety of storage devices.

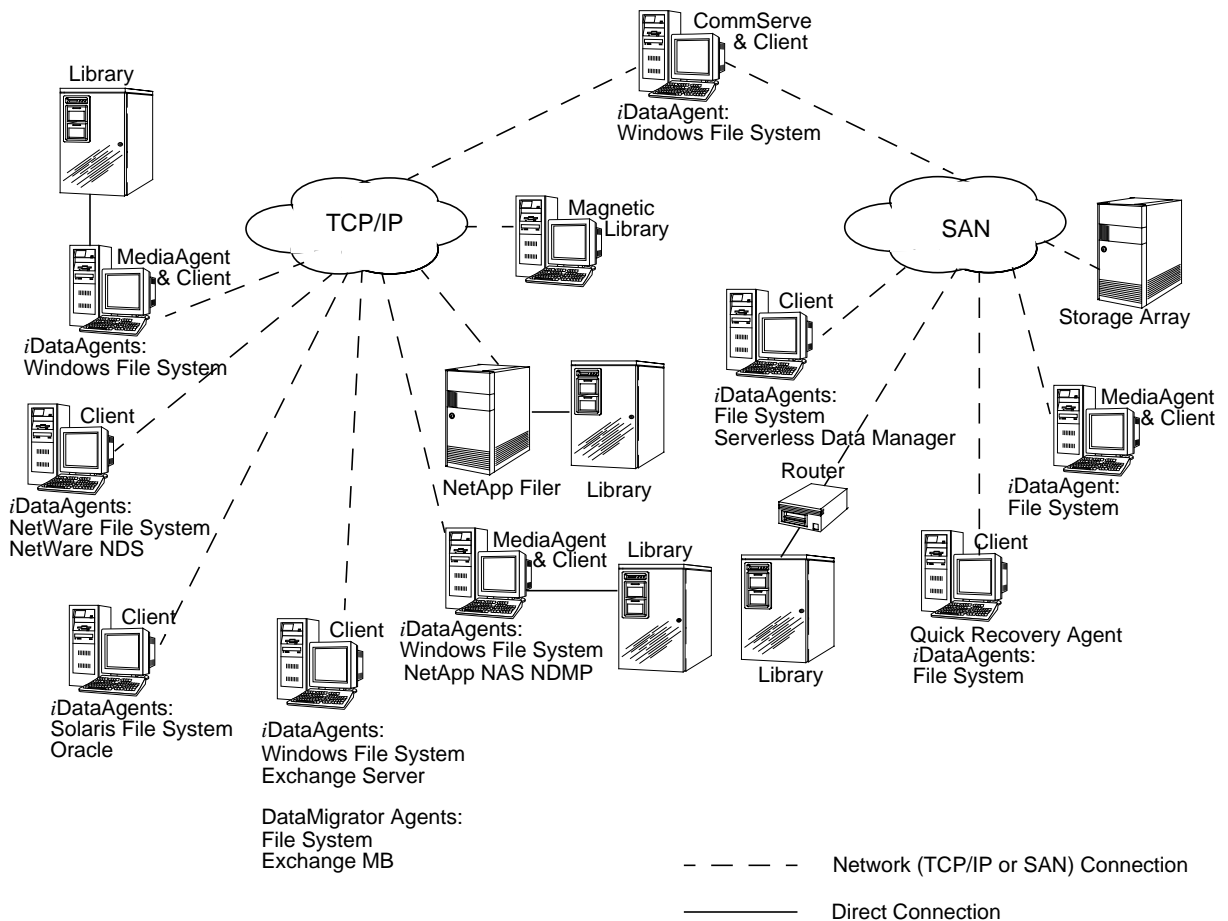
The MediaAgent can also function as a copy manager that leverages other data transfer mechanisms, such as a third party copy. In such cases, the MediaAgent interfaces with the Quick Recovery Agent and Serverless Data Manager to move data.

The following diagram provides a summary of the CommCell components:



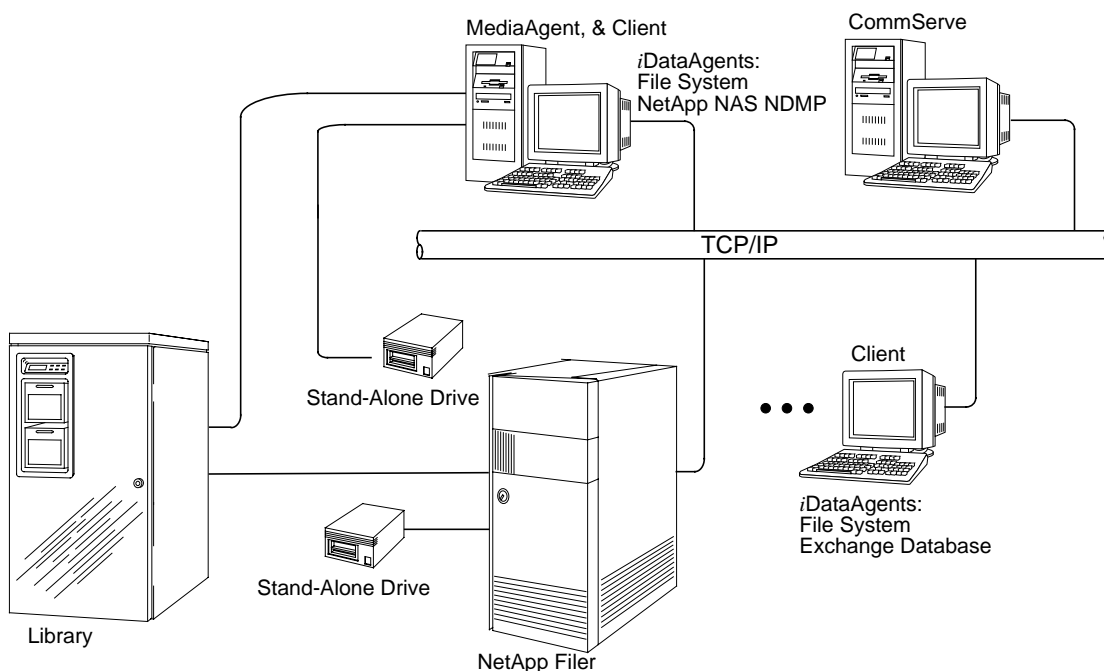
QiNetix Installations

The QiNetix software is modular and can reside on the same and/or separate computers depending on your needs. Some administrators may have a dedicated CommServe computer and a dedicated MediaAgent computer. Others may want to back up the file system data on the CommServe and therefore install the client software on the CommServe computer as well. Still others may use the same computer to serve as the CommServe, MediaAgent, and a client. The QiNetix software supports any and all of these configurations. The following figure shows an example of a CommCell:



What You Need to Know About the NetApp NAS NDMP iDataAgent

The iDataAgent for NetApp NAS NDMP is the backup and restore vehicle for NetApp filer data (i.e., files and folders) residing on the NetApp filer. The NetApp NAS NDMP iDataAgent is just one of several iDataAgents that provide backup and restore support for different kinds of data in what is often a heterogeneous network environment. The following figure shows one such example.



Supported Data Types

The NetApp NAS NDMP iDataAgent supports the backup and restoration of:

- ✦ UNIX qtrees
- ✦ Common Internet File System (CIFS) and Network File System (NFS) qtrees

You can, if desired, back up or restore data with UNIX or Windows NT File System permissions.

What You Need to Know About Galaxy

The Galaxy system is implemented using an extremely flexible architecture. This flexibility enables you to address a broad range of storage management requirements, from dedicated single client storage environments to heterogeneous widely-distributed enterprise environments.

The Galaxy architecture is exposed to you through a robust set of configuration features. During installation, Galaxy establishes a default configuration which may by itself satisfy your storage management requirements. If however, your storage management needs are more unique, you may want to tune certain aspects of the configuration to suit your individual requirements. To perform this task effectively, you need to understand the key aspects of the CommCell architecture, most notably:

- ♦ Subclients
- ♦ NDMP Remote Server
- ♦ Storage policies
- ♦ Backup Sets

Remember, once installed, the Galaxy software is configured to back up all installed clients. You do not necessarily need to change this configuration. If at some later time you decide to change the way a client computer is backed up, then you can always change the CommCell configuration, in whole or in part, at that time.

The rest of this chapter is devoted to explaining the key architectural aspects listed previously. The discussions center primarily on function, but also seek to offer guidance by describing the benefits and limitations of various configuration choices which can be made.

Subclients

A subclient is a portion of a Galaxy client. For clients, it is a designated subset of the client's data. When a client is installed, the Galaxy software automatically creates a default subclient for that client computer. If desired, you can create additional subclients, with each subclient containing a unique portion of the filer.

Subclients fulfill two general purposes. They allow you to:

- ◆ Back up different parts of the system at different times.
- ◆ Back up multiple parts of the system in parallel.

This section and the following describe each of these implementations in greater detail.



User defined subclients are optional and need not be defined provided the default subclient implementation satisfies your backup/restore requirements. The size of the subclient directly impacts the backup and subsequently the restore. The larger the subclient, the longer the time required to backup/restore. Additionally, extra space is needed on the MediaAgent

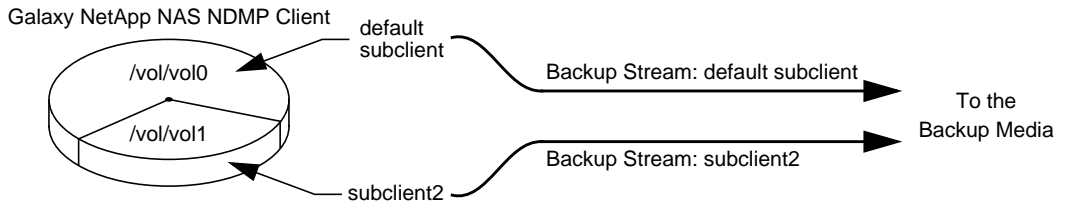
NetApp NAS NDMP iDataAgent

If your default subclient comprises only `/vol/vol0` and you have additional volumes on your filer, you need to create additional subclients for these volumes, in order to backup that portion of the data. The size of your subclient directly impacts the length of time it takes to do a backup and restore. A maximum size of 50-80G per subclient is recommended.

To run most efficiently, the MediaAgent requires memory equal to 0.1% of the total size of data being backed up at any one time. By breaking backup sizes (subclient content) into smaller chunks, the memory requirements on the MediaAgent will be greatly reduced.

Example for NetApp NAS NDMP iDataAgent

The following figure, shows a simple subclient configuration for a filer with two volumes. The default subclient consists of /vol/vol0 and subclient2 comprises /vol/vol1. Each subclient, when it is backed up or restored, establishes a logical channel through which data can travel to or from the backup media.



In this configuration, you can schedule the backups of the default subclient and subclient2 either at different times or simultaneously. Splitting the backups into two time periods can be useful if you need to stage the backups of a large client around a particularly busy time of network or client utilization.

You cannot add multiple content items for a subclient where the content items have case-only differences. Only one of these content items will be saved. Choose a lower level content item that includes both content items. Additionally, you can use two subclients.



Note that while defining subclients you must take care to ensure that the contents of the subclients do not overlap each other. This results in incorrect browsing and thereby inhibits the ability to access and restore backed up data.

If, however, the contents overlap, you can exclude the overlapping portions by using either one of the following two methods:

- ✦ Exclude data using a backup filter.
- ✦ Exclude data using the exclude qtree option.

As you configure the subclient, Galaxy shows you all possible root paths. Add any subdirectories to the root path.

These topics are discussed further in *Excluding Data from Being Backed Up* on page 3-8.

Establishing Parallel Backups Via Subclients

You can schedule multiple subclients for simultaneous backup. This way, the backups proceed in parallel and take less time than if the client was not divided into separate subclients.

Note however that in order for the subclient backups to run in parallel, they must be configured to use either different storage policies or a storage policy that is configured to have at least one data stream for each subclient. If any of the subclients are configured to backup to the same storage policy and that storage policy is not configured for multiple data streams, then resource contention will arise and the competing subclients will back up one after the other. For information on storage policies and data streams, see *Storage Policies* on page 2-13. For details on resource contention see *Hardware-Specific Resource Issues* on page 2-21.

NDMP Remote Server

NDMP Remote Server is an optional software component that allows data from NetApp filers to be backed up to a library attached to a MediaAgent.

To use a library attached to a MediaAgent, the NDMP Remote Server software must be installed on that MediaAgent. Once the NDMP Remote Server software is installed, all storage policies configured on that MediaAgent will be selectable as a backup destination from the NetApp NAS NDMP *iDataAgent* subclient properties Storage Policy Selection screen.

Many Galaxy storage policy features are available when an NDMP Remote Server is installed and the NetApp NAS NDMP *iDataAgent* data is backed up through the MediaAgent, that are not available when backing up data through a NAS-attached storage device.

Storage Policies

A storage policy forms the primary logical entity through which a subclient is backed up. Its chief function is to map backup data to a physical backup media. Although Galaxy automatically creates a default storage policy for every library or stand-alone drive under its control, you can create as many additional storage policies as necessary to properly manage your backup data.

- ◆ If NDMP Remote Server is being used, a storage policy can point towards any MediaAgent Storage Policy or NAS NDMP Storage Policy. If NDMP Remote Server is not being used, a storage policy can only point towards a NAS NDMP storage policy.

Create storage policies to:

- ◆ Customize data retention periods for different subclients.
For example, where it may be necessary to restore old data, you may want to create a storage policy with longer retention periods when backing up data on a server. On the other hand, if the data being backed up is not as critical, you can set a shorter retention period in order to release the media more quickly.
- ◆ Define the number of streams available to subclients to run simultaneous backups or restores for subclients using a specific storage policy.
For example, set a stream count to three and backups from three subclients can run simultaneously rather than in series.
- ◆ Perform an Aux Copy. When you are creating additional copies for a Storage Policy to perform an Aux Copy and the libraries are NAS-attached, the copies have to point to drive pools that are attached to NetApp filers. Similarly, if you are creating additional copies for a Storage Policy to Perform Aux Copy with libraries attached to a MediaAgent, the copies must point to drive pools attached to MediaAgents.

Subclients can be configured to use storage policies using one of the following methods:

- ◆ One storage policy for all types of backups, including full and non-full backups.
- ◆ One storage policy for full backups and another storage policy for non-full backups. The storage policy for non-full backups is referred to as an *Incremental Storage Policy*.

For more information on Storage Policies and Incremental Storage Policies, refer to the *CommServe Administration Guide*.



Because there are differences in the way Galaxy handles different media types, be sure to read the relevant sections within *Hardware-Specific Resource Issues* on page 2-21 before you configure storage policies and copies.

In the next section we discuss a storage policy as a collection of copies.

Copies

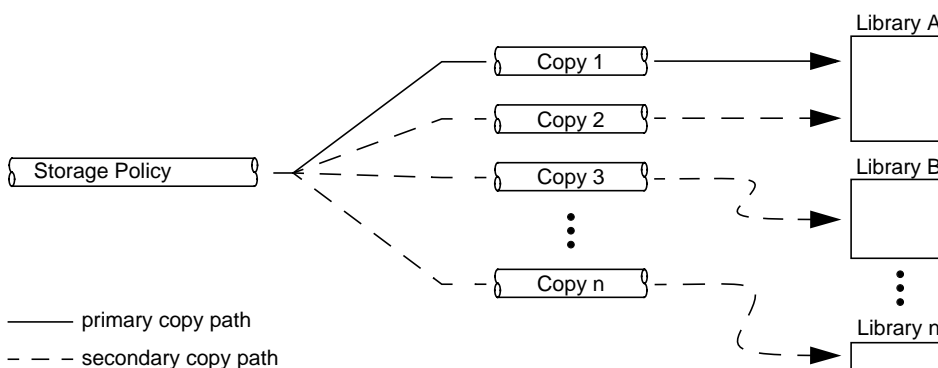
A storage policy consists of one or more copies. The first copy, called the primary, is created automatically by the system when a storage policy is declared. The primary copy carries all the backup data that is directed to the parent storage policy.

In addition to the primary copy, Galaxy allows you to create additional copies for a storage policy. These copies are known as secondary copies. When you are creating additional copies for a Storage Policy to perform an Aux Copy and the libraries are NAS-attached, the copies have to point to drive pools that are attached to NetApp filers. Similarly, if you are creating additional copies for a Storage Policy to Perform Aux Copy with libraries attached to a MediaAgent, the copies must point to drive pools attached to MediaAgents.

When configured, each copy is assigned a set of attributes. These attributes define the nature of any backup that the copy conducts. Such attributes include the:

- ◆ Destination library of the data secured through the copy.
- ◆ Data compression scheme.
- ◆ Data retention period for all data to be secured through the copy.
- ◆ Copy precedence.
- ◆ Copy type (synchronous or selective).

The following figure shows the relationship between primary and secondary copies, libraries, and their parent storage policy.



The types of secondary copies you can create are synchronous and selective copies.

Synchronous Copies

Synchronous copies contain data for all the backups performed on the primary copy when auxiliary copy operations are run. In case data is lost you can restore the same data from the synchronous copy. For more information about synchronous copies, see the *CommServe Administration Guide*.

Selective Copy

Galaxy supports a selective copy feature for storage policy copies when the NDMP remote server is installed. Selective Copies allow you to selectively copy full backup data from primary to selective copies, which provides better tape rotation. The selection process does not have to be the same for all auxiliary copies. The selective copy selection can either be time based or cycle based.



Only full backups can be copied to selective copies. As a result, selective copies cannot be promoted to the primary copy.

Both synchronous and selective copies have several uses, which are discussed in the following sections.

Auxiliary Copy Operations (Jobs)

Galaxy performs backups through the primary copy only. However, you can copy the backup data that was created on a primary copy to all secondary copies within a storage policy, using the auxiliary copy operation. This copies the data as a true image of the primary copy, archive file for archive file. Once the data has been copied, it is available for the length of time specified by the copy's data retention period. (discussed in *Archive Pruning* on page 2-19).

For more information on the auxiliary copy feature, see the *CommServe Administration Guide*.

When using Auxiliary Copy with NDMP Remote Server installed, the Auxiliary Copy uses a storage policy on a MediaAgent that has the NDMP Remote Server installed. When using Auxiliary Copy with a NAS-attached tape drive, the Auxiliary Copy can only be performed from one NAS-attached device to another.

Restore Operations (Jobs)

During a restore operation, Galaxy will search for the requested data from the synchronous storage policy copy with the lowest copy precedence to the synchronous storage policy copy having the highest copy precedence.

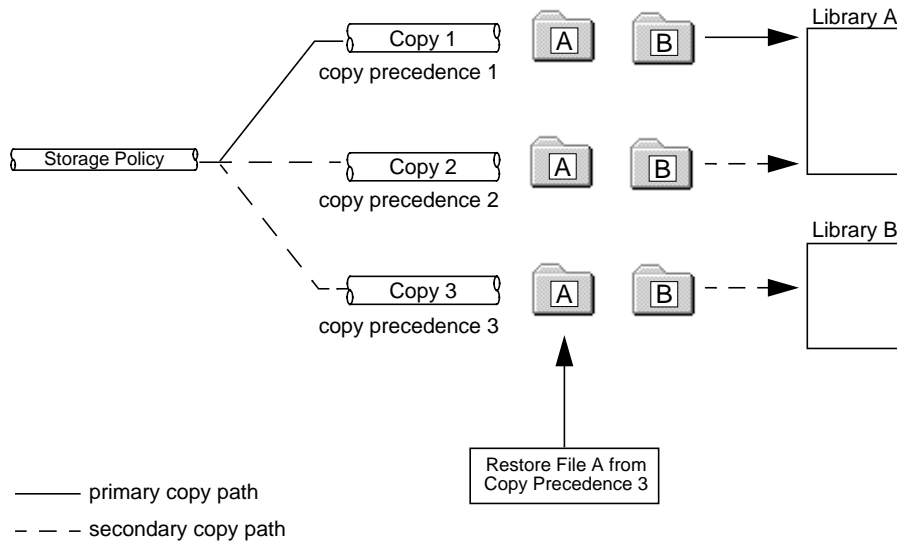
Copy Precedence

When a copy is configured, Galaxy automatically assigns it a copy precedence number, which you can change at any time. When requesting a browse/restore operation, you can specify a copy precedence number from which you want the data restored. This can be useful in several scenarios, including the following:

- ♦ The primary copy is no longer available for restore operations due to a hardware failure.
- ♦ The secondary copy restores from a magnetic disk, which is more efficient than the tape library from which the primary copy restores.

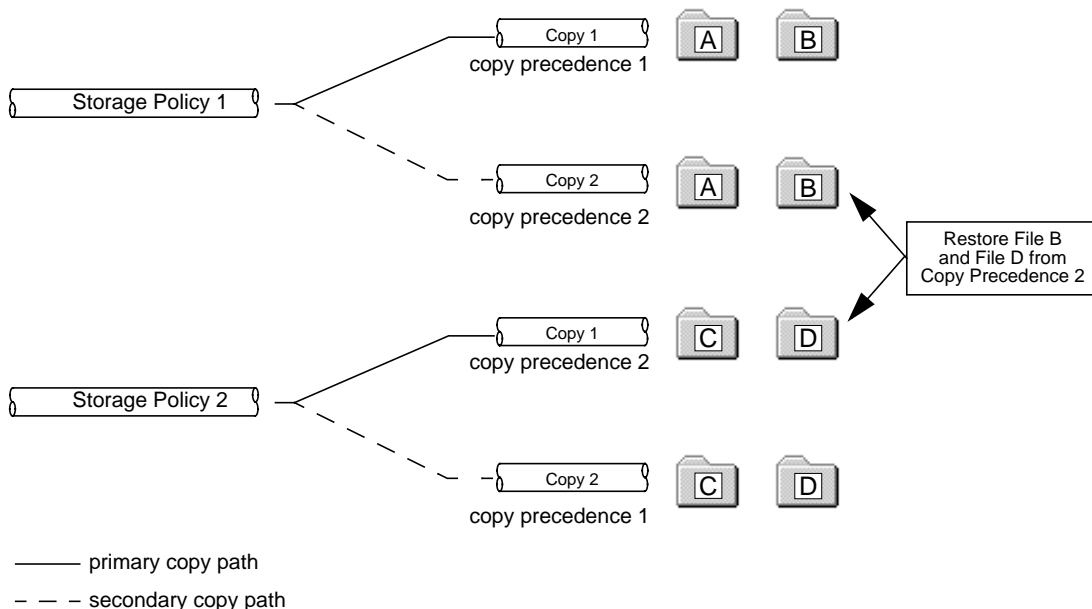
Note that if you attempt to restore from a specific copy precedence and the data is unavailable through the given copy, Galaxy does not search the remaining copies, and the restore operation fails.

The diagram that follows depicts a storage policy that includes three copies. Two of the copies direct data to library A, and the third directs data to Library B. (For simplicity, the copies in the diagram that follows correspond to the copy numbers. In actuality, however, the copy precedence can be changed at any time, and therefore does not necessarily correspond to the copy number.)



In the preceding diagram, restoring from copy precedence 3 forces Galaxy to restore the data from Copy 3 without initially searching the primary copy. If File A is unavailable through Copy 3 (due to data pruning, for example) the restore operation fails.

When you restore from copy precedence, keep in mind that the restore data may have been secured through more than one storage policy, each one associated with more than one copy. If you specify a copy precedence for a restore operation, the data is restored from the specified copy precedence for all of the associated storage policies. If the data is unavailable through the specified copy for any of the storage policies, the restore operation will not complete successfully. This is illustrated in the diagram that follows.



In the above diagram, the data requested was backed up through two different storage policies. Therefore, specifying a copy precedence forces Galaxy to restore from the given copy precedence for both storage policies. Note that if File D is unavailable through Copy 1 (due to data pruning, for example), the restore operation will not complete successfully.

Archive Pruning

Each storage policy copy has configurable parameters called retention time and retention cycles. These parameters determine how much data is retained and for how long. For a cycle to be eligible for pruning, both of its retention time and retention cycles must be exceeded.

The Archive Pruning operation removes data that has exceeded its user-defined retention period while keeping other data intact and available to be restored/recovered. When all the data on a specific media are pruned, that media is automatically recycled back to a scratch pool to be used again by Galaxy for future data protection operations.

Data Retention Periods and Archive Pruning Rules are defined fully in the *Galaxy CommCell Administration Guide*.

In addition to the information provided there, this *iDataAgent* has supplemental archive pruning rules which are explained next.

Archive Pruning Rules for NetApp NAS NDMP *iDataAgent*

For NetApp NAS NDMP *iDataAgent* data, the retention period is defined by three parameters:

- ◆ The length of time.
- ◆ The number of full backup cycles. (A full backup cycle begins with a full backup and includes all other backups up to, but not including the next full backup.)
- ◆ Copy considerations (If you have multiple copies for a Storage Policy, the data should be in sync with each copy.)

Data becomes a candidate for pruning only when all of these thresholds are exceeded for all backups within a full backup cycle. This means that data is pruned only on full backup cycle boundaries and not on an individual backup basis.

The following example demonstrates how NetApp NAS NDMP *iDataAgent* backup data is pruned. Assume that a new subclient is scheduled for backups at 2:00am three times a week. One backup is a full (Fn); the other two are differentials. Since this is a new subclient, no prior backup activity exists. If we assume that the associated data retention period requires that this data be available for 3 full backup cycles and 14 days, then the backup data from the first full backup cycle would become a candidate for pruning only when the F4 full backup completes.



To understand why, consider this explanation. When full backup F1 finishes successfully, the full backup cycle is established. Any subsequent differentials simply add to the cycle. When full backup F2 completes, the F1 and F2 backup cycles are both available. When full backup F3 completes, the F1, F2, and F3 backup cycles are available. When full backup F4 completes, four cycles of backups are available: F1, F2, F3, and F4. This number exceeds the specified number of cycles in the retention period. In addition, the data from the F1 cycle exceeds the 14-day threshold because the 3/6 differential is older than 14 days. Since all the data from this cycle exceeds both retention criteria, it can be deleted by the pruning utility.

Hardware-Specific Resource Issues

Storage policy copies and streams associate logical data entities with physical media. In order to configure storage policies and copies for maximum efficiency, you must understand how Galaxy uses your backup media and the hardware-specific limitations that apply to each media type. For example, you can run multiple operations simultaneously if they are directed to magnetic disk media. However, this may cause resource contention if the jobs are directed to a removable media library, since a given media is only available for one operation at a time. The sections that follow describe issues relating to each type of media supported by Galaxy.

Removable Media Libraries

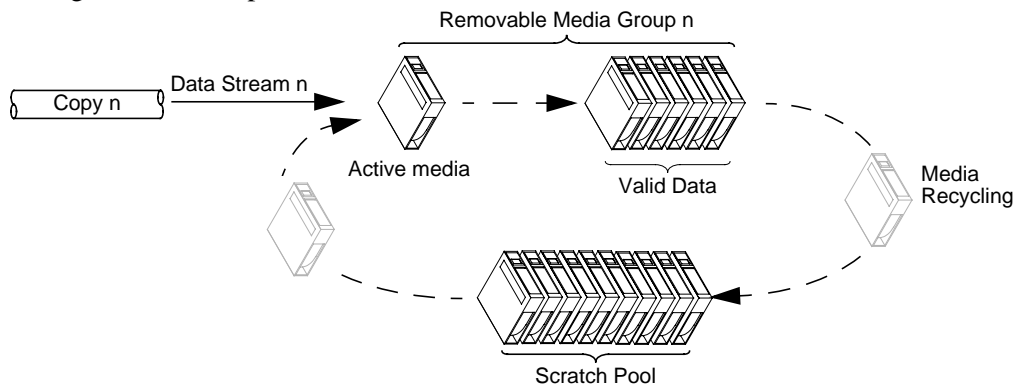
Because removable media (e.g., tape cartridges and optical disks) can only be accessed by one media drive (and consequently one operation) at a time, you must plan carefully to avoid resource contention. The sections that follow explain how contention can arise.

Removable Media Groups

A media group is simply one or more related media to which data is written during a backup. There is a one-to-one correspondence between media groups and data streams. Each time a given stream is in use, it transfers data to or from the same media group. Consequently, the data stored by a media group tends to be from the same subclient(s).

Within a removable media group, only one media (e.g., tape, optical disk, etc.) receives backup data. This media is called the active media. Once the active media reaches capacity, either through one large backup or a series of smaller ones, Galaxy gets a new media from a scratch pool, designating it as the active media. While the original active media still contains valid data, it is no longer used for backup purposes; however, it will

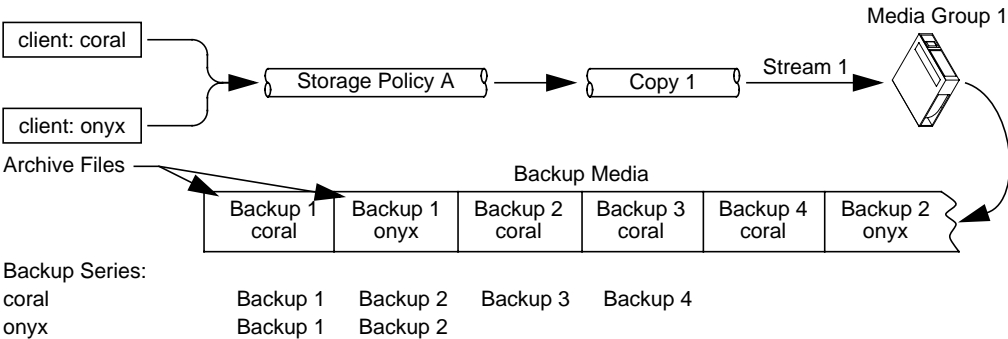
be used if the data it contains is needed for a restore operation. Over time, additional media are cycled through the active state and the media group grows. The size (i.e., the number of media) of the media group depends on the retention period of the copy through which the data backed up and the quantity of data backed up to the media during the retention period.



Backup Series within Removable Media Groups

A removable media group can contain the data of more than one subclient. The data mix, if any, depends on whether the backups of other subclients are mapped to the same storage policy. Since a storage policy has a primary copy, all data sent to that storage policy is ultimately written to the same set of streams; therefore the same media group(s). When the backup data of two or more subclients are mapped to the same storage policy, the destination media group(s) become a composite of different backup series; one backup series per subclient.

Take a simple example in which the backups of two NetApp clients, coral and onyx, are associated with the same storage policy, A, which is associated with a removable media library. Assume no subclients are declared; hence, each client computer comprises only the default subclient. When backups of these subclients are initiated, the backup data is written to the same media group in the form of archive files as shown in the following figure. Each backup produces one archive file. Although the data resides on the same media, the backups retain the identity of their origins thus preserving their integrity for data restoration.



In the previous example, the media group comprised two backup series. If additional subclients were associated with the same storage policy, even subclients from different *iDataAgents* (e.g., for Exchange Database), then the media group would contain one more backup series for each additional subclient.

When you associate subclients with storage policies (and consequently copies), it is important to realize that only one subclient can access a given media at a time. If a media contains multiple backup series, operations that need access to different series on the media cannot run simultaneously. In the example above, a restore of Backup 1 to coral cannot run at the same time as a restore of Backup 2 to onyx.

Media Contention within Removable Media Groups

When you direct the backups from different subclients to the same storage policy, you increase the likelihood of resource contention for those storage policy copies that are associated with removable media libraries. A removable media group can support one operation at a time. As a result, backups or restores that access the same storage policy at the same time may actually be performed serially. This is particularly true if the corresponding storage policy is configured to provide only one data stream. Removable media contention tends to lessen as the number of configured streams increases. Even so, since a given backup can use any stream, it is possible that the backup data for different clients could, over time, be written to the same stream, therefore the same media. Consequently, removable media contention can arise when backing up or restoring data to different clients that share the same storage policy.

Remember, the Galaxy system never compels you to consolidate the data of different subclients or client computers within the same storage policy. To avoid the effects of media contention, you may want to create additional storage policies.

Scratch Pools

A scratch pool is a repository of new and pruned media. Each storage policy copy that is associated with a removable media library is also associated with a scratch pool.

Media cycle through the scratch pool. When a removable media group exhausts the capacity of the active media, it marks the media as full and appropriates another from the scratch pool. Over time and in accordance with the associated retention period, data is pruned by the Galaxy pruning utility. Once all of the data on a given media has been pruned, Galaxy recycles the media by reassigning it from the media group back to the scratch pool where it can be reused. Of course, if the associated retention period is unlimited, the data never expires; consequently, the media never recycles and the size of the media group continues to grow with each backup.

Drive Pools and Resource Contention

A drive pool is a group of drives within a single removable media library that are controlled by a specific MediaAgent. Each storage policy copy that is associated with a removable media library is also associated with a drive pool.

To help you get the most out of your removable media libraries, Galaxy allows you to allocate the arm changer and drives within a library to different MediaAgents and/or NetApp NAS NDMP *iDataAgents* within the CommCell. The system creates a drive pool for all of the drives within a given library that are controlled by a specific MediaAgent or NetApp NAS NDMP *iDataAgent*. (For additional information on library sharing and drive pools, see the *CommCell Media Management Administration Guide*.)

If you divide control of a library's drives among multiple MediaAgents and/or NetApp NAS NDMP *iDataAgents*, you must take the following into account to avoid resource contention:

- ◆ When a library's resources are divided among devices, jobs running via a particular MediaAgent or NetApp NAS NDMP *iDataAgents* can only use drives that are attached to that device. This means that fewer drives are available and resource contention is more likely than if the library were not shared.
- ◆ When you configure storage policies, the number of drives in the smallest drive pool associated with any copy of the storage policy determines the maximum number of streams that can be created simultaneously by any copy of the storage policy.

Magnetic Disk Libraries



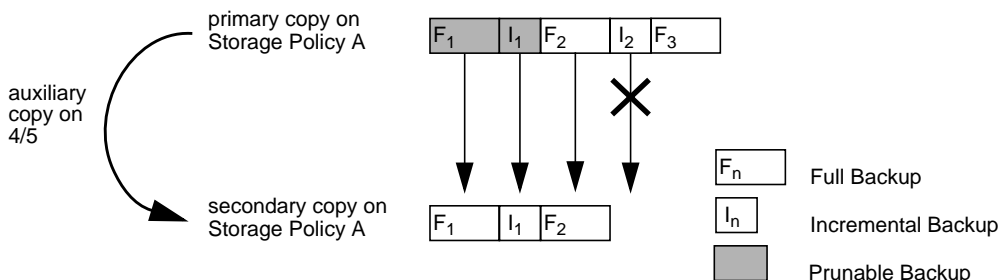
Magnetic disk libraries can be created only for NDMP Remote Server policies.

Theoretically, there is no limit to the number of streams that can access a magnetic disk simultaneously (though if too many simultaneous operations are attempted performance suffers). When you configure a magnetic disk library, Galaxy prompts you for the maximum number of streams that will be allowed to read and write to the library at once. You can set the maximum readers and writers to the highest number that the system can use efficiently, given the system processor, operating system, user load, etc.

Consequently, resource contention is not an issue for a storage policy if all of the storage policy's copies are associated with magnetic disk libraries. Still, all copies of a storage policy must have the same number of streams. If one copy of a storage policy is associated with a magnetic disk library while another copy is associated with a media type that places physical limitations on the number of streams supported (e.g., tape), the copy directed to magnetic disk is subject to those limitations as well.

Media Recycling

If data stored on media exceeds its retention period and the archive pruning utility is run, the data is logically deleted (i.e., removed from the Galaxy database). If all of the data on a medium is pruned, the medium is recycled. That is, it is returned to the scratch pool that is currently associated with the storage policy copy that writes to the medium. In the illustration that follows, two full backup cycles, each consisting of one full and one incremental backup, were written to the primary copy. Subsequently, an auxiliary copy was attempted. The F_1 , I_1 , and F_2 backups were successfully copied to a secondary copy of the storage policy, but the operation failed while copying the I_2 backup.



The only files from the primary copy that can be pruned are those from the F_1 and I_1 backups. Although the F_2 backup was successfully secured by the auxiliary copy, it cannot be pruned because the I_2 backup, which belongs to the same backup cycle, is not eligible for pruning. Files that were backed up as part of the F_2 backup cycle will not be pruned until an auxiliary copy completes successfully, even if they exceed their retention criteria and you run the pruning utility.

For more information on Media Recycling, refer to the *CommCell Media Management Administration Guide*.

Backup Sets

A backup set is a logical grouping of subclients. During client installation, Galaxy creates the default backup set on the client computer. The default backup set always contains a default subclient. You can also create additional subclients within the default backup set. What you create additional backup sets, you lose the ability of performing incremental and differential backups. This applies to all backup sets on that client. When all but one of the backup sets are removed the user once again can do the incrementals and differential backups.

Through the default backup set, you can establish:

- ♦ A backup for a given client computer.
- ♦ A subclient group for a given client computer.
- ♦ A backup for related subclients (i.e., members of a subclient group).

Managing Your Data

This chapter provides an overview of the backup and restore features provided by the NetApp NAS NDMP *iDataAgent*. This information will help you understand the available options so that you can implement efficient backup and restore strategies that meet your storage management requirements.

- ◆ Backup Overview, 3-2
- ◆ Backup Procedures, 3-10
- ◆ Restore Overview, 3-14
- ◆ Restore Procedures, 3-26

Backup Overview

For Galaxy NetApp NAS NDMP *iDataAgents*, the Galaxy system supports:

- ♦ Full backups
- ♦ Incremental backups (with ONTAP version 6.1.1 or higher)
- ♦ Differential backups

These backups can either be scheduled or manually initiated.



Ensure that the NetApp filer has NDMP turned on before you begin the backup. This can be done by executing the command `>ndmp on` from the filer's console window.



NDMP backups are non-interruptible; this means that if a backup of a NAS device is interrupted for any reason, the backup process will need to start again from the beginning. For this reason, a user cannot pause NDMP backups.



The backup size will never equal a sum of the file sizes in a NAS backup. There is a backup header and file headers inserted into the backup file.

Full Backups

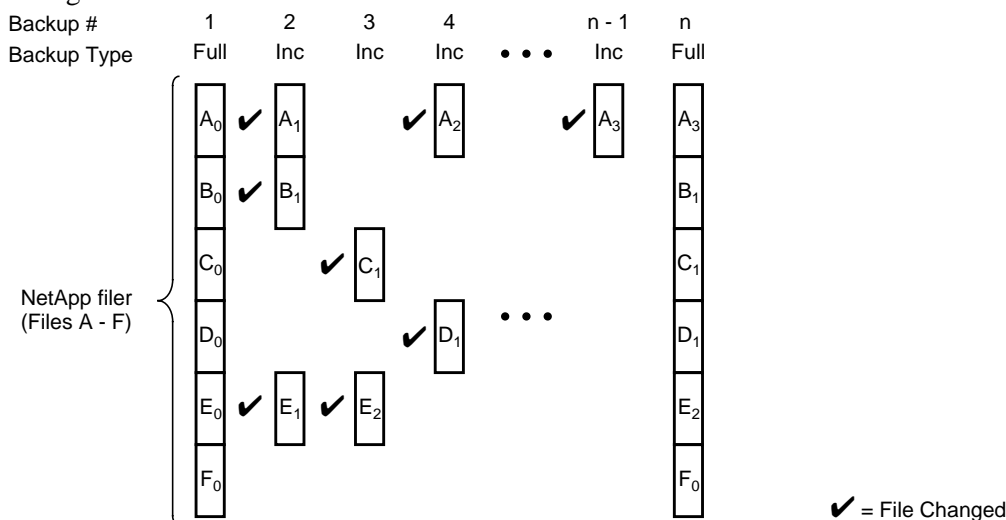
Backups for any client start with a full backup. The full backup becomes a baseline to which subsequent differential and incremental backups are applied, should data restoration be requested.

A full backup contains all the data associated with an *iDataAgent*. It is essentially a snapshot of the client's data. If a client computer has three NetApp NAS NDMP *iDataAgent* subclients in its backup set, then each subclient would need a full backup in order to secure the entire contents of these subclients.

Incremental Backups

An incremental backup contains only those files and directories that have changed since the last backup, regardless of the type. On average, incremental backups consume far less media and place less of a burden on resources than full backups.

The following illustration clarifies the nature of full and incremental backups. For simplicity, assume that there is a NetApp filer that contains six files as represented in the figure.



Backup #1 is a full backup and therefore writes all the data, changed and unchanged, to the backup media. Backups #2 through #n-1 are incrementals and back up only those files that have changed since the time of the last backup, regardless of the type. For example, files A, B, and E changed after the full backup and were therefore backed up in Backup #2. Backup #4 backed up files A and D because both files were modified sometime after Backup #3 occurred. File F did not change; hence, it was not backed up in any of the incremental backups, but it was included in both full backups, which, by definition, back up everything.

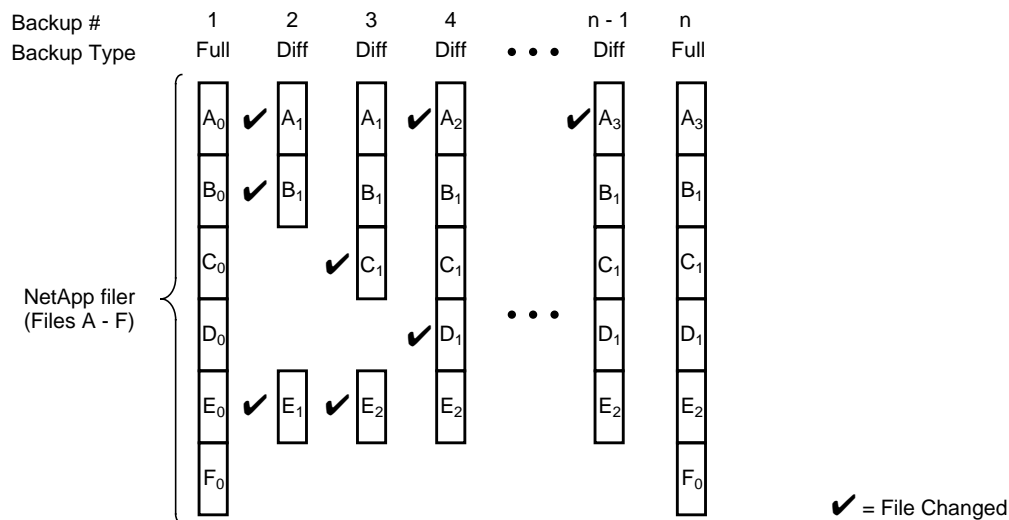


You can perform up to 9 incremental backups after a full backup before another full of differential backup needs to be performed or up to 8 incremental backups after a differential backup before another full of differential backup needs to be performed.

Differential Backups

A differential backup contains only those files and directories that have changed since the last full backup. Differential backups, on average, consume less media and place less of a burden on resources than full backups.

The following illustration demonstrates the nature of differential backups. For simplicity, assume there is a NetApp filer that contains six files as represented in the figure.



Backup #1 is a full backup and therefore writes all the data to the backup media. Backups #2 through #n-1 are differential backups and only back up those files that changed since the time of the last full backup. For example, files A, B, and E changed after the full backup and were therefore backed up in Backup #2 as well as all

subsequent differential backups. File C changed sometime after Backup #2 and was consequently backed up in Backup #3 and all subsequent differential backups. File F did not change; hence, it was not backed up in any of the differential backups, but it was included in both full backups, which, by definition, back up everything.

When a Non-Full Backup is Automatically Converted to a Full Backup

Under the following conditions, a non-full backup is automatically converted to a full backup:

- ◆ If it is the first backup of the subclient.
- ◆ If you re-associate a subclient to another storage policy.
- ◆ If you promote a secondary storage policy copy that is not synchronized with a primary copy (for all the subclients of a storage policy).
- ◆ If a backup job within the most recent backup cycle is pruned or disabled from a primary copy.

For more information on re-associating subclients to another storage policy, the unsynchronized promotion of a secondary storage policy copy, and job based pruning or job based disabling, refer to the *CommServe Administration Guide*.

Scheduled Backups

Scheduled backups provide a convenient means of backing up data without user intervention. You can establish backup schedules for each subclient using the CommCell Console.

When scheduling backups, you need to establish a backup schedule for each subclient. It is recommended that a backup schedule contains a full backup and may contain one or more differential backup. When combined for a given subclient, these backups comprise a full backup cycle.

Full Backup Cycles and Retention Periods

The full backup cycle of a subclient should reflect the retention period of the data. The converse is also true. The backup data is retained in terms of the:

- ◆ Length of time
- ◆ Number of full backup cycles

These concepts are fully described in *Archive Pruning* on page 2-19. The retention period implicitly suggests a relation between the amount of time that you want the data to remain valid and the number of full backup cycles that you expect to complete during that time period. For example, a retention period of 14 days, 2 full cycles suggests that 2 full backup cycles are completed in a time period of 14 days, one full cycle a week. Consequently, for this subclient, it would be appropriate to schedule full backups on a weekly basis.

As another example, a retention period of 28 days, 2 full cycles suggests that 2 full backup cycles are completed in a time period of 28 days, one full cycle every two weeks. It would therefore be appropriate to schedule full backups on a biweekly basis.

As demonstrated by these examples, the full backup cycle (i.e. the length of time between full backups) for subclients, should be established by the ratio of the retention period parameters, specifically;

Length of time/Number of full cycles = Full backup cycle

When to Schedule Backups

A backup, like any other process, consumes system resources. The extent to which any given backup affects other applications depends on several factors:

- ◆ Amount of data to be backed up.
- ◆ Processing power of the client computer.
- ◆ Compression mode of the backup or compression settings on the filer.
- ◆ Number of other backups occurring for the same client computer.

We suggest that you schedule regularly occurring backups for times of low system utilization. For example, you may want to avoid backing up during office hours. If backup data must travel across a network to reach the destination library, then scheduling backups during off-peak hours can be even more important since launching many backups simultaneously could diminish network responsiveness. The extent, if any, to which network responsiveness is degraded depends on a number of issues including the quantity of data being backed up concurrently, capacity of the network, network configuration, etc.

It is often prudent to distribute the scheduled backups in a CommCell over some period of time in order to avoid media drive and media group contention. The length of time for any particular CommCell depends on the amount of data to be backed up and the specific configuration of the CommCell with respect to libraries and storage policies.

If the number of media drives is small compared with the number of subclients in the CommCell, drive contention can occur. If the number of storage policies is small compared with the number of subclients or if a specific storage policy is the target of many subclients, then media group contention can occur. (Media group contention is discussed in *Media Contention within Removable Media Groups* on page 2-24.) If either condition occurs, backups will queue until the needed resource becomes available. Consequently, backups may extend beyond the backup window that was intended for the CommCell.

Backing Up Subclients and the Backup Set

The Galaxy system allows you schedule or initiate backups at either the subclient or backup set level. Selecting the backup set level saves you from having to select the individual subclients. If you select the backup set, Galaxy applies the same schedule or backup request to all constituent subclients.

Remember that the rules for initiating backups of sibling subclients still apply. If the subclients within the backup set are mapped to the same storage policy and that storage policy is not configured for multiple data streams, then Galaxy queues the backups performing one backup operation at a time. This topic is discussed further in *Establishing Parallel Backups Via Subclients* on page 2-11.

Managing the Tapes Where the Data Resides

Start New Media Option

This option starts a new media for your NAS backup data.

Mark Media Full After Successful Backup

This option allows you to mark a tape that contains your NAS data as full after a successful backup and then starts a new tape.



If a backup job needs a new (spare) tape, and if there are no spare tapes available, the backup phase of the job fails, and the job goes to a waiting state. Once the spare tape(s) are made available, the job should complete.

Excluding Data from Being Backed Up

Excluding Data Using the Exclude Qtree Option

While defining the contents of a subclient, you have the option to exclude qtree data for the subclient. Qtrees can be used to exclude entire directories. Use the Subclient Properties to select/deselect the Qtree option. This option can only be selected for subclients who have one content path and that content path is defined at a volume level. If this option is selected, all qtrees on that volume will be excluded from the backup

Excluding Data Using Backup Filters

Each subclient has a backup filter. These filters allow you to specify the data that you want to exclude from a backup. The filters allow you to exclude files whose file names match certain patterns (e.g., *.nsf).

The following list summarizes the rules for filtering files for NetApp NAS NDMP iDataAgent subclients:

- ◆ Name of the file must exactly match the filter string.
- ◆ Asterisk is the only wildcard character.
- ◆ Wildcard character must be the first or last character within the string. Each string may contain a maximum of two wildcard characters.
- ◆ You can specify a maximum of 32 strings in the exclude list.
- ◆ You cannot enter paths as a filter (e.g. /vol/vol0/data1).
- ◆ Data will not be backed up in a differential backup for a subclient after a filter was removed.



You can define filters to exclude qtrees and/or directories from a NetApp NAS NDMP iDataAgent subclient. You must however verify and ensure that the names of such qtrees/directories are unique before you add these names as filters. This would ensure that the filter only excludes the qtrees/directories that you would like to exclude.

Memsaver Option

The NAS backup process can take up a significant amount of virtual memory. A general rule is to have 0.1% of your backup path size available in virtual memory. If you are backing up a subclient whose largest path has a size of 1 terabyte, you should have at least 1 gigabyte of virtual memory available for the NetApp NAS NDMP *iDataAgent*.

Since the NetApp NAS NDMP *iDataAgent* is on the MediaAgent, you should add the NAS memory requirements to the memory requirements of the MediaAgent.

There is a switch (Platform Information/<MachineName>/MediaAgent/sNASMEMSAVER) that allows the NAS backup process to use disk instead of memory. There are still memory requirements for NAS, however they are much lower and the backup will run much slower. It is recommended that you add 256M of virtual memory over the MediaAgent requirements when this flag is turned on.

For information on configuring the memory on a NetApp NAS NDMP *iDataAgent*, see *Registry Keys and Parameters* on page B-1.

Pre/Post User Impersonation for Backup Jobs

When using pre/post commands to execute processes before and after Galaxy backup jobs, you have the option of utilizing the Local System Account or, for added security, assigning a Windows User Account as having permission to run these jobs. The User Impersonation designated for backup jobs is independent of the User Impersonation account you can assign for restore jobs. For more information on Pre/Post Processes and User Accounts, refer to the online help.

Backup Procedures

In this section, we will back up the data from the NetApp filer.

Before You Begin

Review the following to avoid common problems:

- ✦ You have installed the NetApp NAS NDMP *iDataAgent* software on the MediaAgent computer.
- ✦ The MediaAgent computer and the media library are powered on.
- ✦ The NetApp filer is powered on.
- ✦ The CommServe is running.
- ✦ Connectivity to filer from MediaAgent/CommServe

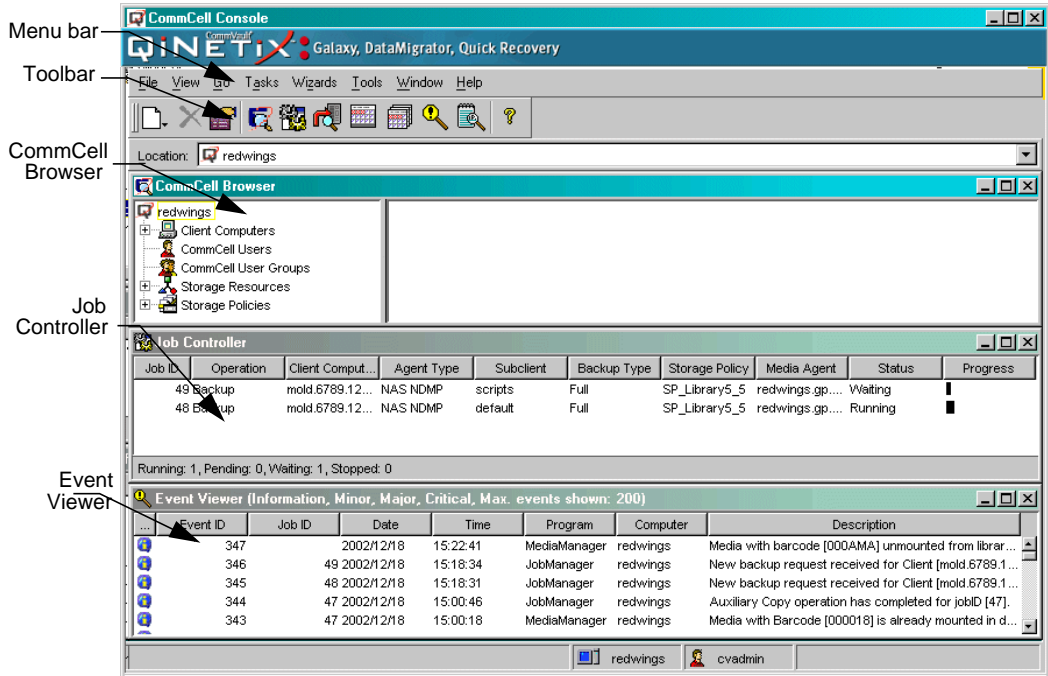
Required Capability: Data Protection Operations

❑ To back up NetApp filer data

Once you have reviewed the *Before You Begin* above, you are ready to back up the data on the NetApp filer.

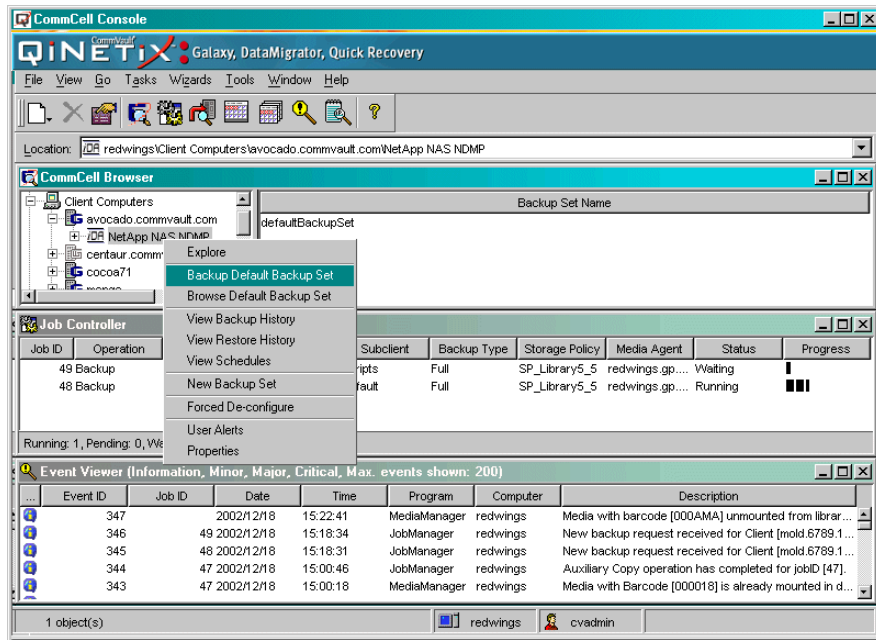
- 1 Log on to the CommServe computer.
- 2 Click the Windows Start button and select Programs -> CommVault
QiNetix -> Galaxy -> CommCell Console for JAVA GUI.
- 3 From the CommCell Logon window, log on by entering your CommCell user name and password.

- 4 Galaxy displays the CommCell Console window.



- 5 From the CommCell Browser, open the Client Computers node, and expand the server whose data you want to back up.

- 6 From the CommCell Browser, right click the *iDataAgent* icon for NetApp NAS NDMP, and then click Backup Default Backup Set from the short-cut menu.



- 7 You are asked to confirm that you want to backup all the subclients within the backup set. Click **Yes**.
- 8 From the Backup Options window click **Run Immediately** and click **Full**, for a full backup, and then click **OK**.



Regardless of the type of backup you select, Galaxy performs a Full backup the first time any backup is started.

- 9 Galaxy starts a full backup of the NetApp filer data and indicates its status in the Job Controller window. (You can track the status by right-clicking the job and then clicking Details. The job status should change from Waiting to Running in a few moments.)



The backup may take a while, depending on the amount of data specified in the subclient contents.

- 10 If you are using a stand-alone drive, Galaxy prompts you to load a specified cartridge into the drive.

If you are not using a stand alone library, you will not receive this prompt. Galaxy loads the tapes automatically. Skip to the next step.



Your cartridges should be labeled with the assigned barcodes. This enables you to locate the correct cartridge for a restore operation, if necessary.

This task is now complete.

Restore Overview

The Galaxy system provides two general operations that help you retrieve backed up data: browse and restore. Additionally, the list media operation helps you to identify the media that may be required. These operations are performed at the backup set level, which allows you to browse and restore data for an entire NetApp filer.

Browsing Data

A browse operation provides a snapshot of the data that has been backed up for the client computer. It does this by retrieving the index file(s) of the related subclient(s) and displaying the results to the CommCell Console. There the NetApp filer structure is graphically displayed, revealing the directories and files that have been backed up. You can use this display to select some or all of the data and restore it using a restore operation.

Restoring Data

The restore operation retrieves the data that you select in the CommCell Console. Galaxy offers a variety of restore options which enable you to restore the data in the manner desired. Note that Galaxy does not require that you browse the data first. If you know the path of the data that you want to restore, you can type it in the Restore window and perform the restore operation directly.

To restore the desired data, you should have a basic understanding of how the Galaxy system restores both files and directories. The following sections describe the restoration process under a variety of circumstances.

Restoring data from a large backup can take a long time. The restore first creates the files to be restored as zero length files and then populates them. If a user of the filer deletes/modifies these zero length files while the restore is processing, the restore will fail. It is recommended that the administrator should shut down the access to the filer while the restore is running to prevent this from happening.

Browse and Restore Scenarios

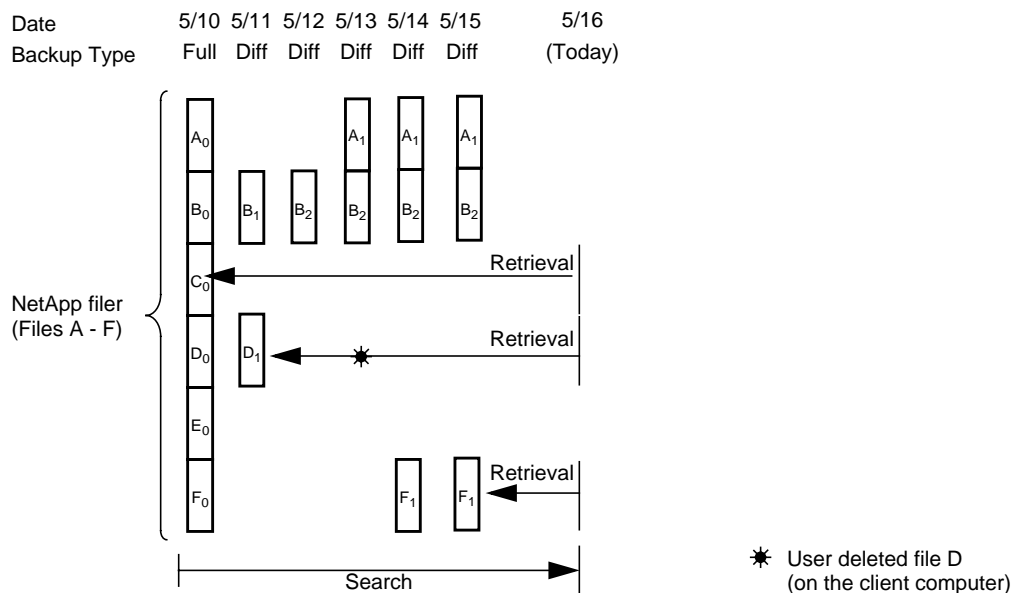
A browse operation displays the NetApp filer structure as it existed as of some specified time. A restore operation restores the data of the NetApp filer or some specified portion thereof.

The following sections examine the browse and restore operations in more detail. Remember, the two operations are the same except that a restore returns the actual data while a browse displays only the structure. The hypothetical NetApp filers shown in the figures are identical and contain six files each. Assume that backups are scheduled daily with the first backup occurring on May 10. (The clock times of the backups are unimportant for our purposes.) The figures show which files have changed and consequently have been backed up over time.

File Retrieval

When you browse or restore data, the system by default returns the requested data based on the latest image available. This is usually the information that most users are interested in. The system does this by using the current date and time as the effective date. The following example discusses how a single file is restored.

Assume that on May 16, we request the most recent version (i.e., the default) of file F. In response, Galaxy retrieves the most recent index file, which was generated by the 5/15 backup and searches the index for the most recent version of the file, which is found in the 5/15 backup. Galaxy then retrieves the file from the backup media and restores it to your client computer.

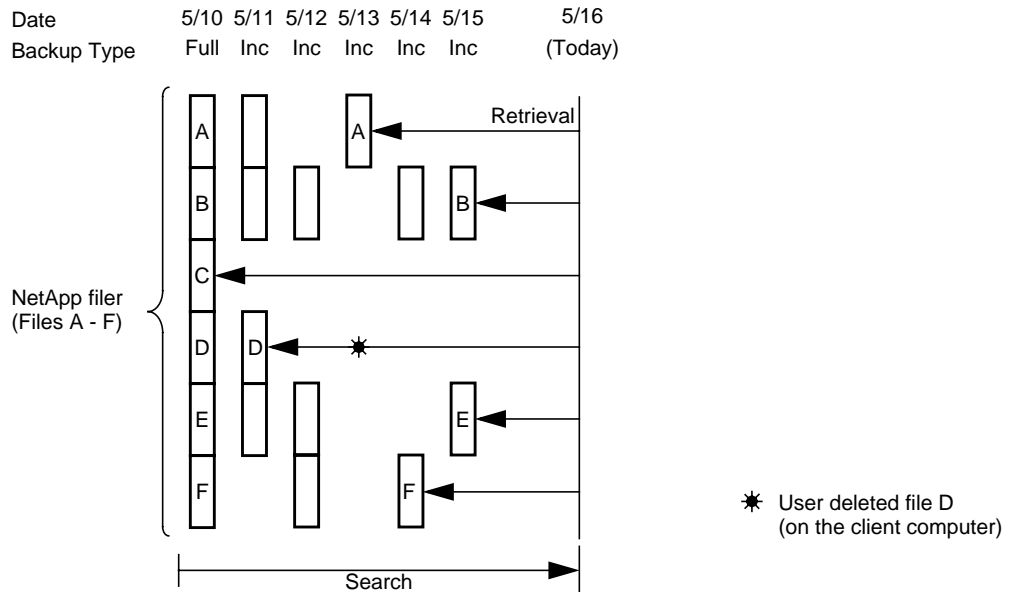


If we requested file C instead, Galaxy would search the index and restore the file version that was backed up with the full backup that occurred on 5/10.

But to request file D, which was deleted from the client's NetApp filer at some time between the 5/11 and 5/12 backups, we would have to begin our search from 5/11 and hence would have to appropriately set the search dates to be able to retrieve the file. (This is described in *Controlling the Browse Time Interval* on page 3-17.)

Directory Retrieval

Assume that on May 16 we request the restoration of a directory (i.e., the entire NetApp filer in this case) as it existed in its most recent state (i.e., the default). Using the latest index file, which was generated by the 5/15 backup, Galaxy retrieves the most recent copy of each file until all the files have been restored.



In this case, the operation would return:

- ✦ Files B and E from 5/15
- ✦ File F from 5/14
- ✦ File A from 5/13
- ✦ File C from 5/10

File D is not restored since it did not exist in the NetApp filer on the date that the restore was effective, 5/16.

Limitations of Default Image Browse/Restore Operation

The default manner of the restore operation (i.e., searching through the current full backup cycle) may not meet your needs in all circumstances. It can only restore the latest version of a file or directory. Further, if the requested file or directory was deleted before the most recent full backup, the default mode of operation cannot find the data.

The Galaxy system provides various restore options which extend its restore capabilities and allow you to control the search and retrieval process. These options are discussed in the following sections.

Controlling the Browse Time Interval

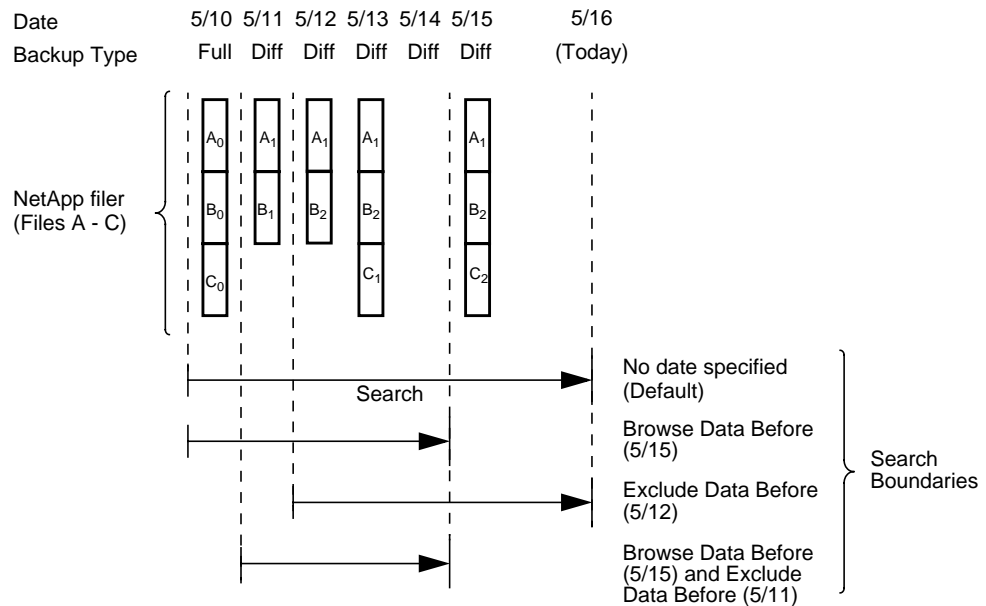
The browse operation provides you with two options, `Exclude Data Before` and `Browse Data Before`, which allow you to control the start and end points of the browse retrieval process. These features can be useful if you need to restore:

- ◆ Some previous version of a file.
- ◆ The contents of a directory as of some earlier date.
- ◆ Data that was deleted prior to the most recent full backup.

Although both options have their uses, the `Browse Data Before` option is generally used far more often than the `Exclude Data Before` option. Users are usually more interested in restoring the most recent data up to some date threshold than they are in omitting data from before some given date.

The `Exclude Data Before` option identifies the starting point of the index search and the `Browse Data Before` option identifies the ending point.

The following figure shows how the search process is affected by the `Exclude data Before` and `Browse Data Before` options.



As shown in the figure, the `Browse Data Before` date, when specified alone, causes the search process to begin with the most recent full backup and end with the backup that occurred just prior to the specified date. The `Exclude Data Before` date, when specified alone, causes the search process to begin with either the backup that occurred just after the specified date or the most recent full backup (whichever is most recent), and end with the most recent backup.

You can also use the `Browse Data Before` and `Exclude Data Before` options together to limit the search boundaries on both ends.

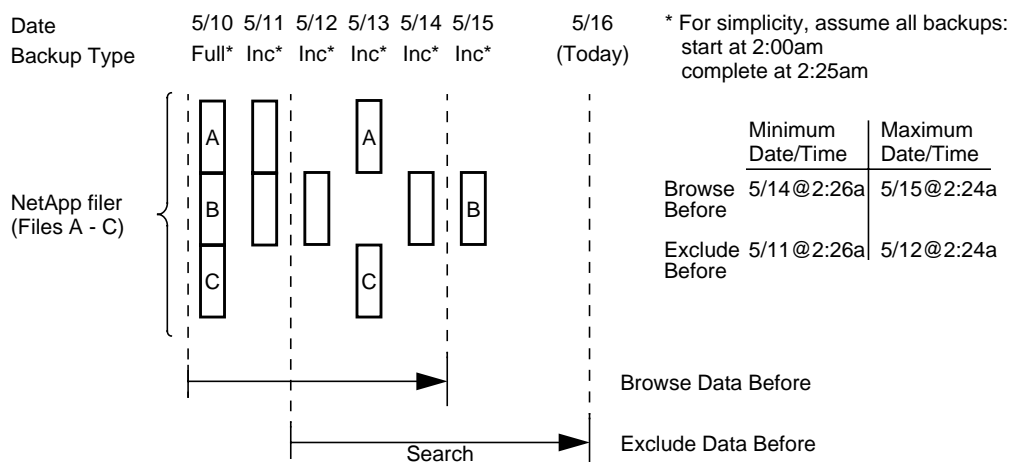
The Time-of-Day Element

The specifications for both the `Browse Data Before` and `Exclude Data Before` options include not only the date, but the time-of-day (i.e., hours and minutes) as well.

Specifying the time is necessary when isolating a backup on a date on which two or more backups occurred. (Note that this condition can occur even if backups are scheduled only once a day. For example, someone may have launched an on-demand backup in addition to a scheduled backup. Also, depending on the size of a backup and the time it is scheduled to begin, a backup can start on one date and complete on the next, since the backup need only span 12:00 midnight.)

In determining whether to include a backup in a search, the Galaxy system uses the time that a backup completes. The `Exclude Data Before` option causes the Galaxy system to begin its search on the backup that completed after the specified date and time, unless it encounters a full backup first. The `Browse Data Before` option causes the Galaxy system to end its browse search using the most recent backup that completed before the specified date and time.

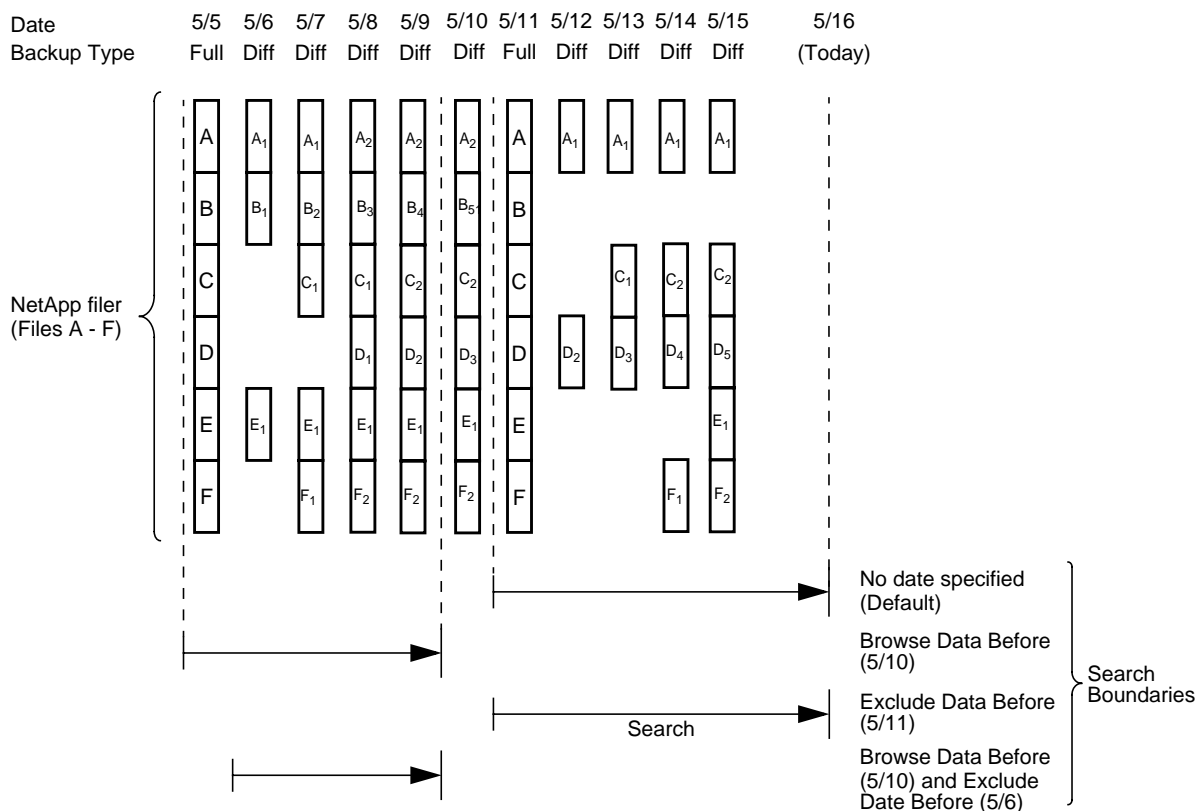
The following figure shows the minimum and maximum times that can be given for the `Browse Data Before` and `Exclude Data Before` options in order to define the search boundaries as shown. Notice that the point of delineation is the backup completion time, 2:25am in this case.



Browsing Data from Before the Most Recent Full Backup

In the browses described previously, the searches are bounded by the most recent full backup. There may be times, however, when you want to browse data that is older than the most recent full backup. The way of accessing that data is to specify a `Browse Data Before` date that pre-dates the full backup. Remember, the `Browse Data Before` date establishes the ending point of the search. Consequently, using a `Browse Data Before` date that pre-dates the most recent full backup starts the search in the previous full backup cycle. This is only valid of course if the data in that full backup cycle has not expired.

The following illustration demonstrates the use of the `Browse Data Before` option to access data that was backed prior to the most recent full backup. Other searches including the default are shown for comparative purposes.



This figure shows that the:

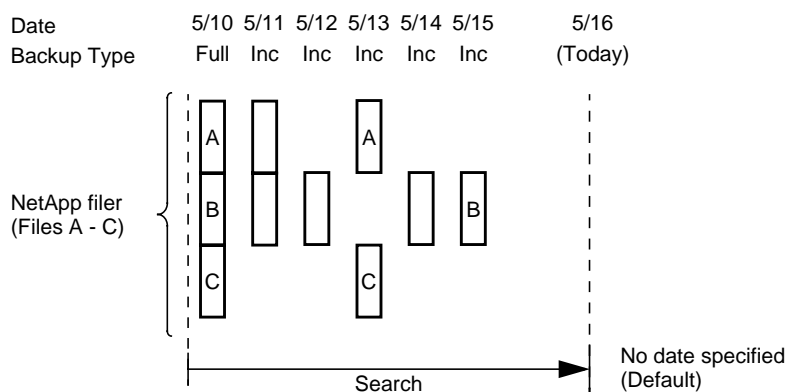
- ◆ Default search is bounded by the most recent full backup. It has no access to data that was backed up prior to that time.
- ◆ `Browse Data Before` option can be used to restore data that was backed up prior to the most recent full backup.

The illustration shows the search boundaries that would be in effect if the date and time specified preceded the completion of the 5/10 backup. The search starts with the 5/9 backup and is bounded by the next most recent full backup.

- ◆ `Exclude Data Before` option, when used alone, cannot access data that was backed-up prior to the most recent full backup, regardless of the date/time that was specified. The end point of such a search is always bounded by either the most recent full backup or the `Exclude Data Before` date, whichever is most recent.
- ◆ Search can begin on a backup that occurred prior to the most recent full backup and end on a backup that occurred after the next most recent full backup.

Browsing Multiple Versions of a File

As part of the default browse operation, the Galaxy system allows you to browse and restore previously backed up versions of a file. You can access this feature by using the `View All Versions` option as described in your online help system. The system responds by displaying the date-stamped versions of the selected file that are available for restoration. You then select the version you want and restore it. The following example demonstrates the use of this feature.



A default image browse of this NetApp filer returns:

- ◆ File A from 5/13

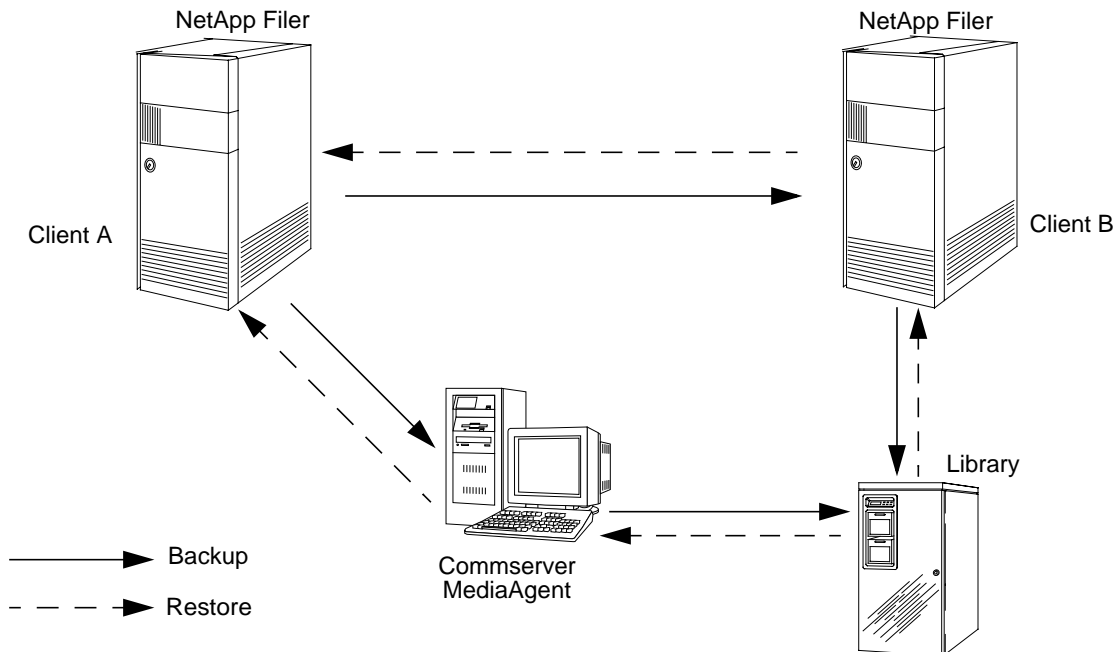
- ◆ File B from 5/15
- ◆ File C from 5/13

Using the `View All Versions` option, we can also browse and restore any version of these files back to the 5/10 full backup. For example, for File A, we can restore the 5/10, 5/11, and 5/13 versions.

Note that this feature is available only for individual files. It cannot be used to restore some previous version of a directory. If you need to restore a directory to some prior state, use the `Browse Data Before` option as described in *Controlling the Browse Time Interval* on page 3-17.

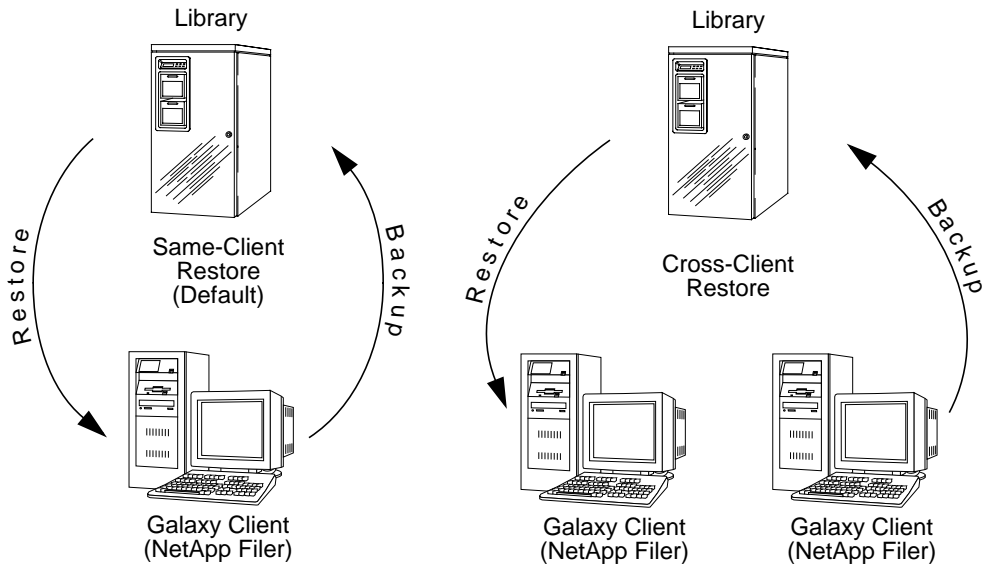
Three-way Backup and Restore Operations

You can also back up and restore data for NetApp filers without a locally attached tape drive, to a storage device attached to another NetApp filer. This three-way backup and restore process allows many filers to share a single, centrally located tape library, or even back up their data to a remote site.



Cross-Client Restore Operations

By default, Galaxy restores data to the client computer from which it originated. If you want, you can also restore the data to some other NetApp device, as long as this NetApp device is also a Galaxy client. This is called a cross-client restore.



- ◆ The restore destination must be on another NetApp Filer within the same organization and site that is configured as a Galaxy client and is operational.
- ◆ Galaxy restore user management capabilities are required on both the source and destination computer in order to perform a cross-machine restore.
- ◆ Note that when you perform a cross-client restore, the restored data assumes the NetApp permissions that it had originally and the Windows NT security attributes (permissions) of the parent directory.

File System NDMP Restore Operations

A file system NDMP restore is another form of cross-client restore. With a file system NDMP restore, the data is restored to a computer with a different operating system. Galaxy supports the following file system NDMP restore operations:

- ◆ NetApp NAS NDMP to Windows type file systems

When restoring data from NDMP to a file system, you should be aware of how the data is restored under certain circumstances. Whenever data is restored to an environment from which it did not originate, the data does not always assume its original characteristics.

For more information, refer to *Appendix G, File System NDMP Restore Enabler*

Direct Access Restore

Direct Access Restore allows you to restore data quickly. In a normal restore operation, a large portion of the data from the backup that included the file must be read. In a Direct Access Restore, only the portion of the tape which contains the data to be restored is read.



We recommend using NDMP version 3 with 6.1.2R1. NDMP version 3 is the default with ONTAP 6.1.2.



Direct Access Restore only works on a filer that is ONTAP version 6.0 or higher. If you try a Direct Access Restore on a filer that is 5.3.7R1 or earlier, it can cause the filer to crash.



Unless the NetApp filer is running ONTAP version 6.4, the Direct Access Restore operation is converted to a normal restore when a directory is selected as part of the restore.

Efficient Non-DAR Restore

If the most recent copy of the data that you are restoring was backed up by an incremental or differential backup, the restore only reads the archive file from that differential or incremental backup. Galaxy will not read all the archive files back to the last full backup.

Scheduled Restore Operations

When you want to restore data, you usually need it immediately. However, there may be times when you need the data by some specific time, but not necessarily right away. For example, perhaps you need to restore some data that you do not intend to use until the following day.

Using the scheduling feature, you can schedule a restore operation. As with scheduled backups, a scheduled restore operation relieves you of having to manually initiate the operation. This feature can be particularly useful if you want to restore a large amount of data, but would prefer to do so at a time when either the client computer is not in use or at a time when network utilization is low (assuming the data must travel a network). For details on scheduling a restore operation, see your online help system.

Auxiliary Copy

In a NAS environment, you must be aware of two scenarios in creating copies for the Storage Policy.

- ◆ Libraries attached to a MediaAgent - copies for the Storage Policy must be pointed to drive pools connected to a MediaAgent.
- ◆ Libraries attached to a NetApp device - copies for the Storage Policy must be pointed to drive pools connected to a NAS-attached device.

For details on the Auxiliary Copy operation, refer to the *CommServe Administration Guide*.

List Media Operation

When you want to browse and/or restore data, you can ensure that the media containing the backup data is available for the operation using the list media feature. This feature is also useful to identify media associated with alternate copies of the data. For details on the List Media operation, see your online help system.

Restore Procedures

In this section, we will restore some of the data that you backed up previously. So as to not interfere with existing data, we will restore the data to an alternate path.

Before You Begin

Review the following to avoid common problems:

- ♦ The client computer is powered on.
- ♦ You've successfully done a backup of this client computer.

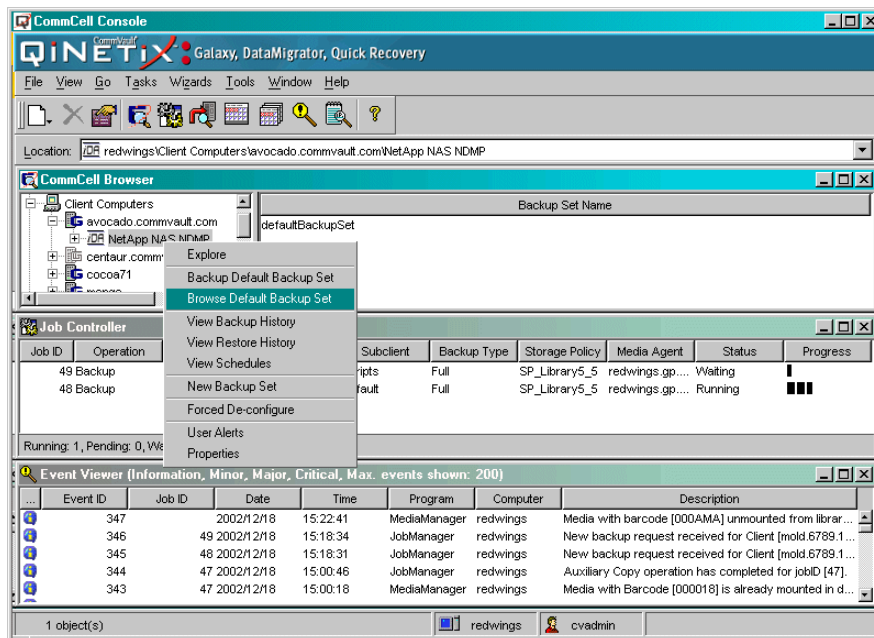
Required Capability: Browse & Recover

❑ To restore NetApp filer data

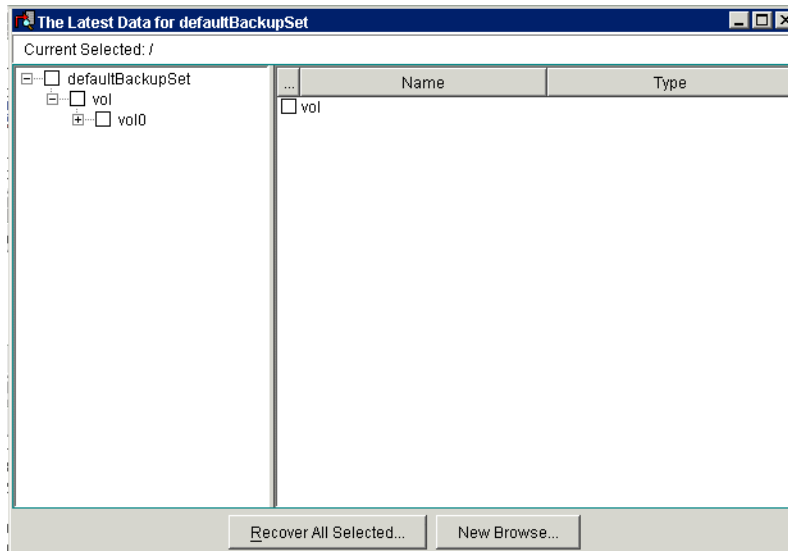
Once you have reviewed *Before You Begin* above, you are ready to restore the data to a NetApp filer.

- 1 Log on to the CommServe computer.
- 2 Click the Windows Start button and select Programs -> CommVault QiNetix -> Galaxy -> CommCell Console for JAVA GUI.
- 3 From the CommCell Logon window, log on by entering your CommCell user name and password.
- 4 Galaxy displays the CommCell Console window.
- 5 From the CommCell Browser, open the Client Computers node, and expand the server whose data you want to restore.

- 6 Right-click the *iDataAgent* icon for NetApp NAS NDMP, and then click Browse Default Backup Set.



- 7 From the Browse Options dialog box, click OK. (We will use the default settings.)
- 8 The Browse window appears, which shows the files and directories that you backed up from the client computer.
- 9 From the Browse window, open the filer structure and select the data you want to restore.
- 10 Click Recover All Selected.



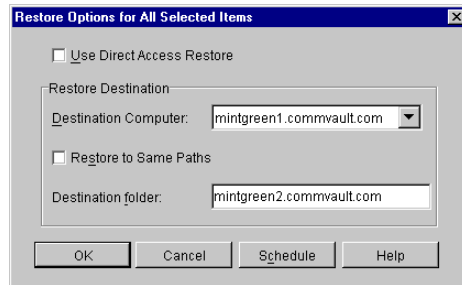
- 11 From the Restore Options dialog box, clear the Restore to Same Paths option, and then type a new path in the Destination folder field. The data can also be restored to an alternate destination NetApp filer.



Although you are entering an alternate, and possibly new path, you must ensure that the root directory already exists on the destination computer, or the restore will fail.



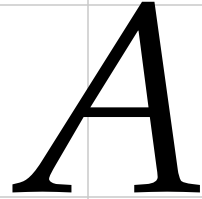
To use the NDMP Restore Enabler feature to restore data to a file system client, select that client as the destination computer. You are required to enter a destination folder. You can use the browse feature to select this destination folder on the target computer. For more information on the NDMP Restore Enabler feature refer to *File System NDMP Restore Operations* on page 3-23 and *File System NDMP Restore Enabler* on page G-1



Click OK. (We will leave the other settings unchanged.) A window to track the progress of the restore operation is displayed.

12 Click OK and verify that the data was restored.

This task is now complete.



Removing the Galaxy Client Software

This appendix describes the procedures used to deconfigure the NetApp NAS NDMP iDataAgent from Galaxy, remove the NetApp NAS NDMP iDataAgent software, and delete the NetApp NAS NDMP icon from the CommCell Console.

This appendix contains:

- ◆ Overview, A-2
- ◆ Deconfiguring a NetApp NAS NDMP iDataAgent from the NAS Client Wizard, A-3
- ◆ Uninstalling the NetApp NAS NDMP iDataAgent Software, A-5
- ◆ Deleting the NetApp NAS NDMP iDataAgent Icon from the CommCell Browser, A-7

Overview

Removing the NetApp NAS NDMP *iDataAgent* is a three-phase process.

- ✦ First you need to deconfigure the NetApp NAS NDMP *iDataAgent* using the Client Wizard.
- ✦ Next you need to uninstall the NetApp NAS NDMP *iDataAgent* software from the MediaAgent computer hosting the software.
- ✦ Finally, you need to delete the *iDataAgent* icon from the CommCell Browser.



Once you uninstall the software, Galaxy can no longer provide NetApp NAS NDMP *iDataAgent backup* services for the NetApp filer.



If you are unable to remove a NetApp NAS NDMP *iDataAgent* from a Galaxy client computer by using the procedures in this appendix, you can use the Forced De-configure feature to release the license and clean up entries from the CommServe database. However, the files and registry entries relating to the *iDataAgent* will not be removed from its host computer. For information and procedures on using Forced De-configure, refer to *Forced De-configure* in the online help.

Deconfiguring a NetApp NAS NDMP *iDataAgent* from the NAS Client Wizard

This section describes how to de-configure a NetApp NAS NDMP *iDataAgent* using the NAS Client Wizard.

Before You Begin

Review the following to avoid common problems:

- ♦ Verify that no jobs are in progress or scheduled to occur while the software is being uninstalled. If jobs are scheduled, either perform the uninstall at another time or disable the jobs on the client computer using the CommCell Console.
- ♦ Verify that the CommCell Console is closed.
- ♦ Verify that the Galaxy Service Control Manager window is closed.

☐ To remove the NetApp NAS NDMP *iDataAgent* via the NAS Client Wizard

Once you have reviewed *Before You Begin* above, you are ready to uninstall the Galaxy NetApp NAS NDMP *iDataAgent* software.

- 1 At the CommCell Console, select `Tools -> NAS Client Configuration`.
- 2 In the NAS Client Configuration window, select the name of the NAS client you want to remove.
- 3 Click `Remove a NAS Client`.



To add this NetApp NAS NDMP *iDataAgent* in the future, the `Undelete` command allows you to re-enable the deconfigured NetApp NAS NDMP *iDataAgent*.

- 4 Verify that a license becomes available when you deconfigure the client. To do this, right-click the CommServe icon in the CommCell Browser, click License Administration, and from the list that is displayed, find the name of the NetApp NAS NDMP *iDataAgent* whose clients you deconfigured. The number of licenses in use for that *iDataAgent* should have decreased by the number of clients you deconfigured.

- 5 Click `Exit`.

At this point, the NetApp NAS NDMP *iDataAgent* icon for this client is disabled in the CommCell Browser, and you can no longer back up data from the deconfigured clients. However, you can restore data to another NetApp NAS NDMP *iDataAgent* in the CommCell.

Uninstalling the NetApp NAS NDMP *iDataAgent* Software

If you remove the NetApp NAS NDMP *iDataAgent* software, all files are removed and no NAS operations can be performed. All data is subsequently lost.

You can remove the NetApp NAS NDMP *iDataAgent* software from your client computer as you would any other application, by using the `Add/Remove Programs Utility` in the Windows Control Panel. The following procedure guides you through this process.

Before You Begin

Review the following to avoid common problems:

- ✦ Verify that no jobs are in progress or scheduled to occur while the software is being uninstalled. If jobs are scheduled, either perform the uninstall at another time or disable the jobs on the client computer using the CommCell Console.
- ✦ Verify that the CommCell Console is closed.
- ✦ Verify that the Galaxy Service Control Manager window is closed.

☐ To uninstall the NetApp NAS NDMP *iDataAgent* software

Once you have reviewed *Before You Begin* above, you are ready to uninstall the Galaxy NetApp NAS NDMP *iDataAgent* software.

- 1 Log on to the client computer as local Administrator or as a member of the Administrators group on that computer.
- 2 Open the `Add/Remove Programs` icon in Windows Control Panel.
- 3 From the `Add/Remove Programs` dialog box, select the `Galaxy NAS iDataAgent`. Note that in Windows NT, this dialog box is called `Add/Remove Programs Properties`.
- 4 Click `Remove` to uninstall the software. Click `Yes` to continue. Note that in Windows NT, this button is called `Add/Remove`.
- 5 The program prompts you to confirm the software removal.

A Removing the Galaxy Client Software

- 6 Click **Yes**. The progress indicator is shown.
- 7 The **NAS Client Configuration** window is shown.
- 8 Highlight the name of a NAS client displayed in the **NAS Client** list and click **Remove a NAS Client**.
- 9 Repeat this procedure until all NAS clients are uninstalled.
- 10 Click **Exit**.



Once you have uninstalled the *iDataAgent*, the corresponding icon in the **CommCell Browser** is marked for deletion (appears dimmed). While this icon exists, you can restore data from the *iDataAgent* to another client. If you delete this icon, all of the *iDataAgent*'s backup data is irretrievably lost.

Deleting the NetApp NAS NDMP *iDataAgent* Icon from the CommCell Browser

After you first deconfigure the client in the NAS client wizard, you can:

- ♦ Leave the corresponding backup data intact for restore purposes.
- ♦ Remove the backup data immediately.

If you delete a NetApp NAS NDMP *iDataAgent* icon, all data for that filer is permanently removed and it cannot be restored.



Once you delete the *iDataAgent* icon from the CommCell Browser, the data for that client cannot be restored. Do not use this option if you want to restore data in the future.

☐ To delete the NetApp NAS NDMP *iDataAgent* icon from the CommCell Browser

- 1 From the CommCell Browser, right-click the NetApp NAS NDMP *iDataAgent* icon that you want to delete, and then click `Delete` from the short-cut menu.



If the delete command is not available, then you have not successfully de-configured and/or uninstalled the *iDataAgent*.

- 2 Click `Yes` to delete the *iDataAgent* icon. The *iDataAgent* icon is removed from the view.

B

Registry Keys and Parameters

This appendix describes registry keys and parameters that can be used with the NetApp NAS NDMP *iDataAgent*.

This appendix contains:

- ◆ Overview, B-2
- ◆ Registry Keys and Parameters, B-1

Overview

The following section describes standard and optional registry rekeys and parameters for the NetApp NAS NDMP *iDataAgent*. These can often be used for advanced troubleshooting or environment-specific modifications. Standard registry keys and parameters are created during the Galaxy installation. Optional registry keys and parameters are manually created by the user. Information is supplied when necessary for key and parameter noting whether it is standard or optional.



Using Registry Editor incorrectly can cause serious problems that may require you to reinstall your operating system. CommVault cannot guarantee that problems resulting from the incorrect use of Registry Editor can be solved. Use Registry Editor at your own risk.



Before you edit the registry, you should back up the registry. You must also understand how to restore it if a problem occurs. For information on how to backup and restore the registry, refer to the appropriate Registry Help Topic provided in `Regedit.exe` or `Regedt32.exe`.

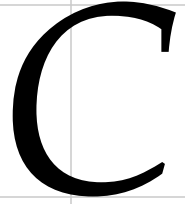
Registry Keys and Parameters

The following registry key may be used on the NetApp NAS NDMP *iDataAgent*.

Location	HKEY_LOCAL_MACHINE\SOFTWARE\CommVault Systems\Galaxy\Platform Information\<MachineName>\MediaAgent
Key	MediaAgent (standard)
Parameter	nIndexDays (standard)
Value Type	DWORD
Valid Range	Number in days
Default Value	15 (Days)
Description	This registry key is used to remove any index cache (for the subclient) which has not been accessed in the specified number of days.

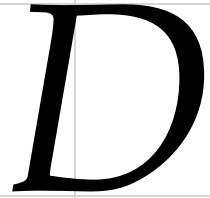
Location	HKEY_LOCAL_MACHINE\SOFTWARE\CommVault Systems\Galaxy\Platform Information\<MachineName>\MediaAgent
Key	MediaAgent (standard)
Parameter	nIndexPercent (standard)
Value Type	DWORD
Valid Range	A percentage, e.g. 90 (To use ninety percent)
Default Value	90 (percent) Setting a value of 0% or 100% indicates that disk full percentage should be ignored during cleanup.
Description	This registry key is used to remove the index cache when the amount of data in the disk housing the index cache is more than the established percentage. During the cleanup, index cache removal will continue until the disk full percentage is less than or equal to the established percentage.

Location	HKEY_LOCAL_MACHINE\SOFTWARE\CommVault Systems\Galaxy\Platform Information\<MachineName>\MediaAgent
Key	MediaAgent (standard)
Parameter	sNASMEMSAVER (optional)
Value Type	String
Valid Range	Y or y (case insensitive)
Description	<p>Used to lower the memory requirements for a NAS backup in the MediaAgent. When enabled, this registry key allows the NAS backup process to use disk instead of memory.</p> <p>Once the key is created, the changes take effect during the following backup operation.</p>



Upgrading the Galaxy Client Software

For information on upgrading the NetApp NAS NDMP iDataAgent software, see the *CommCell Upgrade Guide*.



Obtaining Information from the NetApp Filer

This appendix describes the NetApp procedures for obtaining the NAS NDMP server device names and drive access paths.

This chapter contains:

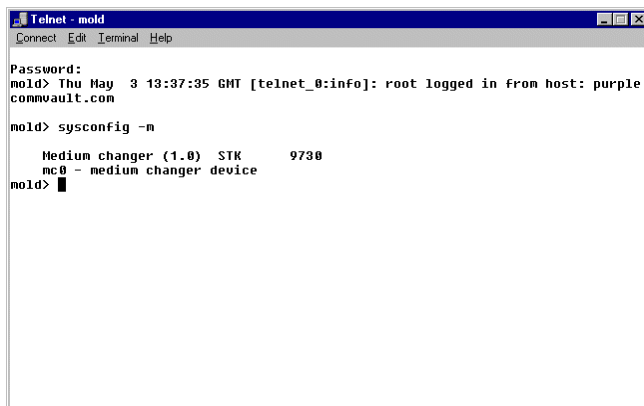
- ◆ Obtaining the Device Name of Media Changer, D-2
- ◆ Obtaining the Drive Access Path, D-3

Obtaining the Device Name of Media Changer



This information is NetApp-specific and is subject to change.

- 1 Use either the web-based administration GUI, filer console, or telnet session to issue commands on the filer.
- 2 Run the `sysconfig -m` command from the filer's console or telnet session. This should display the media changers device name, similar to the information displayed in the following screen.



```
Telnet - mold
Connect Edit Terminal Help

Password:
mold> Thu May 3 13:37:35 GMT [telnet_0:info]: root logged in from host: purple.
commvault.com

mold> sysconfig -m

      Medium changer (1.0)  STK      9738
      mc0 - medium changer device
mold> █
```

In this example, the NDMP server device name is mc0.

Obtaining the Drive Access Path

The NAS NDMP Server Drive Path is the path through which the NetApp filer communicates with NDMP drives. This communication is necessary when backup and restore operations are being performed. You must have the path available when you are adding NDMP drives.



NOTE

This information is NetApp-specific and is subject to change.

- 1 Use either the web-based administration GUI, filer console, or telnet session to issue commands on the filer.
- 2 Run the `sysconfig -t` command from the filer's console or telnet session. This should display the tape drive access path information, similar to the information displayed below. Note that this filer has three drives attached to it.

```

C:\WINNT\System32\telnet.exe

ursth - unload/reload device, format is: 85937 bpi 50 GB (w/comp)
rstth - rewind device, format is: 85937 bpi 70 GB (w/comp)
nrsth - no rewind device, format is: 85937 bpi 70 GB (w/comp)
ursth - unload/reload device, format is: 85937 bpi 70 GB (w/comp)

Tape drive (0b.1) Quantum DLT7000
rst3l - rewind device, format is: 81633 bpi 40 GB (w/comp)
nrst3l - no rewind device, format is: 81633 bpi 40 GB (w/comp)
ursth - unload/reload device, format is: 81633 bpi 40 GB (w/comp)
rst3m - rewind device, format is: 85937 bpi 35 GB (w/comp)
nrst3m - no rewind device, format is: 85937 bpi 35 GB (w/comp)
ursth - unload/reload device, format is: 85937 bpi 35 GB (w/comp)
rst3h - rewind device, format is: 85937 bpi 50 GB (w/comp)
nrst3h - no rewind device, format is: 85937 bpi 50 GB (w/comp)
ursth - unload/reload device, format is: 85937 bpi 50 GB (w/comp)
rst3a - rewind device, format is: 85937 bpi 70 GB (w/comp)
nrst3a - no rewind device, format is: 85937 bpi 70 GB (w/comp)
ursth - unload/reload device, format is: 85937 bpi 70 GB (w/comp)

Tape drive (6.6L1) Quantum DLT7000
rst6l - rewind device, format is: 81633 bpi 40 GB (w/comp)
nrst6l - no rewind device, format is: 81633 bpi 40 GB (w/comp)
ursth - unload/reload device, format is: 81633 bpi 40 GB (w/comp)
rst6m - rewind device, format is: 85937 bpi 35 GB (w/comp)
nrst6m - no rewind device, format is: 85937 bpi 35 GB (w/comp)
ursth - unload/reload device, format is: 85937 bpi 35 GB (w/comp)
rst6h - rewind device, format is: 85937 bpi 50 GB (w/comp)
nrst6h - no rewind device, format is: 85937 bpi 50 GB (w/comp)
ursth - unload/reload device, format is: 85937 bpi 50 GB (w/comp)
rst6a - rewind device, format is: 85937 bpi 70 GB (w/comp)
nrst6a - no rewind device, format is: 85937 bpi 70 GB (w/comp)
ursth - unload/reload device, format is: 85937 bpi 70 GB (w/comp)

Tape drive (6.6L2) Quantum DLT7000
rst7l - rewind device, format is: 81633 bpi 40 GB (w/comp)
nrst7l - no rewind device, format is: 81633 bpi 40 GB (w/comp)
ursth - unload/reload device, format is: 81633 bpi 40 GB (w/comp)
rst7m - rewind device, format is: 85937 bpi 35 GB (w/comp)
nrst7m - no rewind device, format is: 85937 bpi 35 GB (w/comp)
ursth - unload/reload device, format is: 85937 bpi 35 GB (w/comp)
rst7h - rewind device, format is: 85937 bpi 50 GB (w/comp)
nrst7h - no rewind device, format is: 85937 bpi 50 GB (w/comp)
ursth - unload/reload device, format is: 85937 bpi 50 GB (w/comp)
rst7a - rewind device, format is: 85937 bpi 70 GB (w/comp)
nrst7a - no rewind device, format is: 85937 bpi 70 GB (w/comp)
ursth - unload/reload device, format is: 85937 bpi 70 GB (w/comp)

avocado>

```

Use these prefixes to manually configure the drives in a library attached to the NetApp filer

Use these prefixes to configure drives attached to a library in the SAN environment

- 3 You need to select one of the available tape devices which are prefixed with the character “n” and indicated as `no rewind device`. This indicates that when an application closes the tape device, it will not automatically rewind the tape. This is an important requirement for Galaxy. Each tape drive is also suffixed with one of the following density modes used to write to a tape:

“l” for low density

“m” for media density

“h” for high density

“a” for high density with hardware compression

The number refers to the instance - zero normally corresponds to the first tape drive.

- 4 For a library which is directly attached to a NetApp filer, the drives can be configured using the prefixes listed under `Tape Drives` with `<0b.1>` suffix.

For library in the SAN environment, the drives can be configured using the prefixes listed under the `Tape Drives` with the `<6.6L>` suffix.



NetApp NAS NDMP *iDataAgent* only supports `no rewind device` configurations.

E

NAS Disaster Recovery

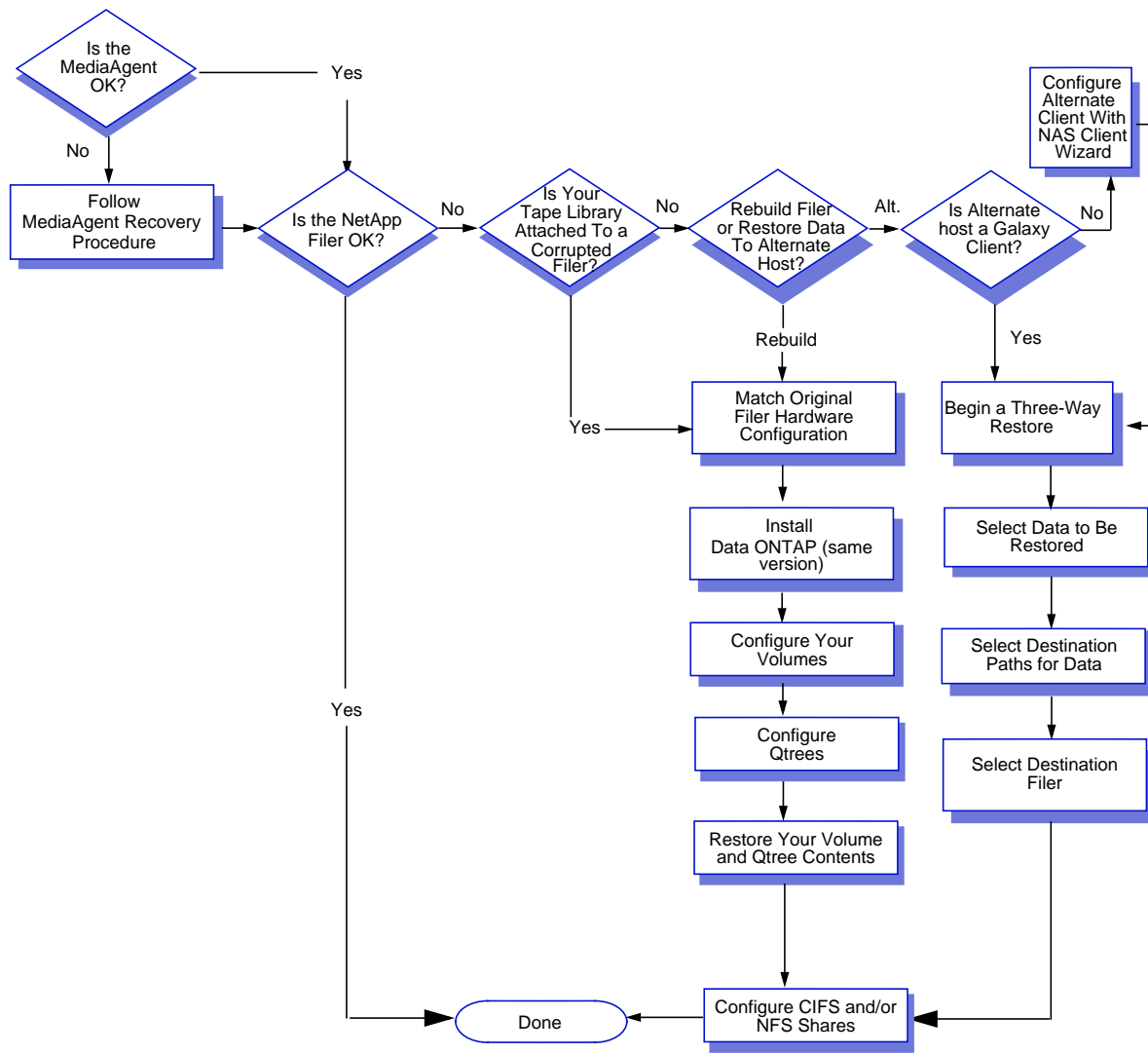
This appendix provides information and procedures for fully restoring a NetApp NAS NDMP iDataAgent computer.

This appendix contains:

- ◆ NAS Disaster Recovery, E-2
- ◆ Performing the Recovery, E-3

NAS Disaster Recovery

The following chart is an overview of performing a NAS disaster recovery on your NetApp NAS NDMP iDataAgent computer. For more information, refer to Performing the Recovery on page B-3.



Performing the Recovery

Overview

This section contains procedures for restoring your NetApp filer. It contains information in the following two sections:

- ◆ Using the Same NetApp Filer - Rebuilding a Filer Using the Original Configuration Options
- ◆ Using a New NetApp Filer - Restoring Your Data to a Different Filer in a Three-Way Restore

Before You Begin

Ensure the following before restoring a NetApp filer or restoring your data to another filer:



If you are restoring to the same filer make sure that you restore to the same configuration settings as the original filer. Make sure you have the same configuration information as your original before you start NAS disaster recovery.

- ◆ The target computer has the same fully qualified network name as the original.
- ◆ You have the same login and password for your NDMP account.
- ◆ Try to match the general hardware configuration of the original filer model and disk shelf configuration.
- ◆ If your filer is connected to a library, make sure that you can match the original physical connections between the filer and the library.
- ◆ If you have a tape drive connected to the filer, make sure that you have the same type of tape drive to that of the original (i.e., DLT 7000, EXB 8900)
- ◆ Match the local volume configuration and number of volumes to that of the original.
- ◆ Match the number and type (i.e., unix, ntfs, mixed) of qtrees to that of the original.
- ◆ Your volumes have the same storage capacity as that of the original (or greater).

Using the Same NetApp Filer - Rebuilding a Filer Using the Original Configuration Options

❑ To rebuild a filer using the same configuration options

Once you have read *Before You Begin* on page E-3, you are ready to rebuild the filer.

- 1 If your filer is connected to a library, set up the new physical connections of your filer to match the original.
- 2 Ensure that your current hardware configuration matches that of the original. If your filer was connected to a tape drive or library, ensure that your tape drive or library has the same settings as the original. If it does not, do the following:
 - a) Select `Galaxy Library and Drive Configuration`.
 - b) Right click the appropriate tape drive (or library).
 - c) Select the correct drive type and type the correct access path.
- 3 Load the same version of the operating system `Data ONTAP` to your filer.
- 4 Run the `sysconfig -t` command to ensure that the names of your tape drives match the access paths of your originals.
- 5 Configure your filer using the `Setup` command.



You must have the same host name, login name, and password as your original filer.

- 6 If you want to reconfigure a filer to masquerade as the original one with the same host name, change the login and password. To do this:
 - a) Enter a CommCell console.
 - b) Click the filer that you are restoring.
 - c) Right-click the NetApp NAS NDMP *iDataAgent* and then click `Properties`.
 - d) Click `Change Account`.

- e) Change the password and login information to match those of the original filer.
 - f) Click **OK**.
 - 7** Use the volume commands to configure your RAID arrays. Your volumes must be of the same number and size as the originals to accommodate the restored data.
 - 8** Use the `Qtree` command to recreate your original qtrees.
 - 9** Make sure that NDMP is enabled on the filer. This can be done in the following two ways:
 - a) From a filer command line run the `ndmpd on` command. You must then edit the `/etc/rc` file on the filer and add the command to the end of the file. This ensures that NDMP will be enabled each time the filer is rebooted.
 - b) From a standard web browser, enter the url: `http://<filer name>/na_admin`. Login using your login and password. Select **NDMP**. Click **Enable NDMP**. NDMP is now enabled and will start automatically each time the filer is booted.
 - 10** Start restoring your volumes and qtrees.
 - 11** Run the `cifs setup` command if you need to configure CIFS shares.
 - 12** Run the `nfs setup` command if you need to export NFS shares.
- You have now completed your full system restore operation.

Using a New NetApp Filer - Restoring Your Data to a Different Filer in a Three-Way Restore

☐ **To perform a three-way restore of your data to another filer**

Once you have read *Before You Begin* on page E-3, you are ready to perform a three-way restore.

- 1** If the destination filer is not already a Galaxy client, setup a new NetApp NAS NDMP *iDataAgent* in the Galaxy NAS client wizard.



The act of configuring a new NetApp NAS NDMP *iDataAgent* consumes a license. You may want to delete the old filer to free up a license. However, do not delete the old client until its files have been restored.

You may want to keep the old client in Galaxy until you are sure that its backup archives will no longer be needed. For example, if your site policy requires a six month retention of backups, then you must keep the old client configuration for six months.

- 2 Right-click the default backup set from the original filer name, then click `Browse Backup Data`.
- 3 From the `Browse Options` dialog box, select the browse options that you want to use and click `OK`.
- 4 In the `Browse` window, open the structure of the NetApp filer tree and select the data you want to restore.



Do not restore data to the `/`, `/vol/vol0/` or `/etc` directories. Doing so will overwrite your configuration data. If `/vol/vol0/` contained user data that must be restored, restore the qtrees or subdirectories individually.

- 5 Click `Recover All Selected`.
- 6 From the `Restore Options` dialog box, select `Restore to Same Paths` if you would like to restore the data with the same path in which it was backed up. If you would like to restore the data to a different path, type the new path in the `Destination Folder` field.
- 7 Select the name of the destination filer from the `Destination Computer` list.
- 8 Click `OK`. You can track the progress of the restore in the `Job Controller`.

You have now completed the three-way restore operation.

Enabling NDMP Service

This appendix provides information on enabling the NDMP service by default in the NetApp filer.

This appendix contains:

- ◆ Enabling the NDMP Service, F-2

Enabling the NDMP Service

After attaching the NetApp filer and MediaAgent machine to the library and before you begin your Galaxy installation, verify that the NDMP service is enabled in the NetApp filer. This is not enabled by default.

You can do this by connecting to your NetApp filer using the filer console or telnet session and issuing the `ndmpd status` command. This will tell you whether the NDMP status is `on` or `off`. If the NDMP service is not enabled, enable the service by executing the command `ndmpd on` from the filer console or telnet session.

To keep NDMP service permanently enabled, add the `ndmpd on` command at the end of the system startup script available in `/etc/rc`. This will automatically enable the NDMP service every time the NetApp filer is booted.

You can also permanently enable the service using an internet browser with the following address:

`http://<filer name>/na_admin`

Click on `Filer View`. This will prompt you for the filer name and password. Use your administrator login and password. Open the `Filer` tree and click on `Misc`. Select `Yes` from the `NDMP Enabled` list.



File System NDMP Restore Enabler

This appendix provides information and procedures on using the File System NDMP Restore Enabler.

This appendix contains:

- ◆ Overview, G-2
- ◆ Install the File System NDMP Restore Enabler, G-3
- ◆ Restore Data with File System NDMP Restore Enabler, G-5
- ◆ Uninstall the File System NDMP Restore Enabler, G-6

Overview

The File System NDMP Restore Enabler allows NAS data to be restored to a Windows computer. The File System NDMP Restore Enabler requires that the CommServe, MediaAgent, File System *iDataAgent* and the NetApp NAS NDMP *iDataAgent* be installed.

You must have an available license for this *iDataAgent*.



You cannot have the NDMP Remote Server and the File System NDMP Restore Enabler installed on the same client.



Unix data that could not exist on a Windows computer, e.g., files that have ‘case only’ differences, might not be restored correctly to the Windows machine

Install the File System NDMP Restore Enabler

Before You Begin

Review the following to avoid common problems:

- ✦ Close all applications and disable any programs that run automatically, including antivirus, screen savers and operating system utilities. Some of the programs, including many antivirus software, may be running as a service. Stop and disable such services before you begin. You can re-enable them after the installation.
- ✦ The client satisfies the minimum requirements provided in the *System Requirements* on page 1-4.
- ✦ The CommServe and MediaAgent are running.
- ✦ If the CommServe, MediaAgent and/or Client are communicating across firewall(s), ensure that ports 8400 and 8402 are allowed connections through the firewall for these computers.
- ✦ You have an available license on the CommServe for the File System NDMP Remote Enabler *iDataAgent*.

To Install the File System NDMP Restore Enabler

Once you have reviewed Before You Begin above, you are ready to install the File System NDMP Restore Enabler.

If you have not installed the Windows File System *iDataAgent*, the install program will automatically install the *iDataAgent* when you select the NDMP Remote Enable. For information on installing Windows File System *iDataAgent* refer to the *Galaxy Client Installation and Administration Guide (Windows File Systems)*. The following procedure describes the steps involved in installing the File System NDMP Restore Enabler only.

- 1 Log on to the computer where the File System NDMP Restore Enabler will be installed, as local Administrator or as a member of the local Administrators group on that computer.
- 2 Place the QiNetix components CD-ROM for the appropriate Windows platform into the client's CD-ROM drive or a mapped CD-ROM drive on another computer. After a few seconds, the installation menu appears.

If the installation menu does not appear:

- a) Click `Start` on the Windows task bar, and then click `Run`.
- b) Browse the CD-ROM drive, right-click `Setup.exe` then click `Open`. From the installation menu, click `Install Galaxy Platforms` on this computer.
- 3 From the installation menu, click `Install Galaxy Platforms` on this computer.
- 4 From the `Welcome` screen, click `Next` to continue if no other applications are running.
- 5 Click `OK` to continue if virus scanning is disabled.
- 6 Read the license agreement. Select `I accept the terms in the license agreement` then click `Next` to continue.
- 7 From the `Select Platforms` dialog box, expand the `iDataAgent` module and select the `File System NDMP Restore Enabler`.
- 8 A summary of the installation options that you have chosen appears. Click `Next` to continue or `Back` to change any option.

Setup now starts copying the File System `iDataAgent` software to the computer. This step may take several minutes to complete.
- 9 Click `Finish` to close the `Setup Complete` dialog box.

Restore Data with File System NDMP Restore Enabler

Restoring data with the File System NDMP Restore Enabler works in the same manner as any other restore operation.

Refer to *Restore Procedures* on page 3-26 for details.

Uninstall the File System NDMP Restore Enabler

This section describes the procedures used to uninstall the File System NDMP Restore Enabler.

Before You Begin

Review the following to avoid common problems:

- ✦ Verify that no jobs are in progress or scheduled to occur while the software is being uninstalled. If jobs are scheduled, either perform the uninstall at another time or disable the jobs on the client computer using the CommCell Console.
- ✦ Verify that the CommCell Console is closed.
- ✦ Verify that the Galaxy Service Control Manager window is closed.

❑ To Uninstall the File System NDMP Restore Enabler

Once you have reviewed *Before You Begin* above, you are ready to uninstall the Galaxy File System NDMP Restore Enabler.

- 1 On the Start menu, click Settings, Control Panel and Add/Remove Programs.
- 2 Select Galaxy File System NDMP Restore Enabler and click Remove.
- 3 The system prompts to confirm that you want to remove the File System NDMP Restore Enabler. Click Yes.

The system removes the File System NDMP Restore Enabler.

Index

A

- active media 2-21
- archive file 2-16
- archive pruning
 - definition 2-20
 - when data exceeds retention period 2-26
- auxiliary copy
 - definition 2-16
 - use in NAS environment 3-25

B

- backup operations
 - convert to full backup 3-5
 - differential backups 3-4
 - full backups 3-2
 - incremental backups 3-3
 - parallel backups 2-11
 - pre/post user impersonation 3-9
 - scheduled backups 3-5
 - three-way backups 3-22
- backup series 2-22
- backup set 2-27
- browsing data
 - before the most recent full backup 3-20
 - controlling the browse time interval 3-17
 - definition 3-14
 - multiple versions of a file 3-21
 - see restoring data
 - transparent full 3-21

C

- client 1-3
- CommCell 1-10
- Common Internet File System 2-7
- CommServe 1-10
- conventions, document Pref-vi
- copy precedence 2-17
- copy type
 - selective 2-15
 - synchronous 2-15
- cross-platform restores 3-23

D

- data types, supported 2-7
- device name of media changer
 - obtaining D-2
- differential backup
 - definition 3-4
 - efficient non-DAR restore 3-24
- direct access restore 3-24
- directory retrieval 3-16
- drive access path
 - definition 1-3
 - obtaining D-3

E

- efficient non-DAR restore 3-24
- excluding data

Index

- using backup filters 3-8
- using Qtree option 3-8
- exhaustive detection 1-25

F

- fibre channel 1-5
- file retrieval 3-15
- file system NDMP restore 3-23
- filtering rules for backup 3-8
- forced deconfigure A-2
- full backup 3-2

H

- hardware installation
 - verifying 1-8

I

- iDataAgent
 - de-configure using NAS client wizard A-3
 - icon removal A-7
 - uninstalling A-5
- incremental backup
 - definition 3-3
 - efficient non-DAR restore 3-24
 - limits on 3-4
 - requirements 1-5
- install
 - NDMP Remote Agent H-3
 - NetApp NAS NDMP iDataAgent on Windows
 - 1-12 - 1-16
 - NetApp NAS NDMP on Unix 1-16
 - requirements 1-4

L

- list media operation 3-25

M

- mark media full 3-7
- media group
 - contention 2-24
 - definition 2-21
 - scratch pool 2-24
- media recycling 2-26
- MediaAgent 1-10
- memsaver option 3-9

N

- NAS disaster recovery F-2
- NDMP
 - adding/configuring drives 1-23
 - drive access path 1-3
 - enabling service G-2
 - remote server 1-3
 - server device name 1-3, D-1, G-1, H-1
- NetApp filer data
 - back up procedure 3-10 - 3-13
 - restore procedure 3-26 - 3-29
- NetApp NAS NDMP iDataAgent
 - install on Unix 1-16
 - install on Windows 1-12
 - what you need to know 2-7
- Network File System 2-7

O

- ONTAP 1-5

P

- pre/post user impersonation 3-9

Q

- QiNetix architecture 2-2
- qtrees
 - definition 3-8

R

- rebuilding a filer F-4
- recovery
 - using a new NetApp filer F-5
 - using the same NetApp filer F-4
- reference documentation Pref-vi
- registry keys E-2
- remote server 1-3
- restoring data
 - cross-client 3-23
 - cross-platform 3-23
 - definition 3-14
 - direct access restore 3-24
 - directory retrieval 3-16
 - efficient non-DAR 3-24
 - file retrieval 3-15
 - limitations of default image 3-17
 - three-way 3-22
 - time-of-day element 3-19
- retention period
 - parameters 2-20

S

- SAN 1-5
- scheduled backup
 - definition 3-5
 - when to schedule backups 3-6
- scratch pool 2-24
- secondary copy
 - copy precedence 2-17
- selective copy 2-16
- server device name
 - definition 1-3
 - obtaining D-2
- stand-alone drive
 - configuring 1-39
- start new media option 3-7
- storage policy
 - copies of 2-15
 - definition 2-13
 - in a NAS environment 3-25

- media groups 2-21
- subclient
 - and backup set 2-27
 - and scheduled backups 3-5
 - definition 2-9
 - use in parallel backups 2-11
- system requirements 1-4

T

- TCP/IP 1-5
- telnet session D-2
- three-way backup/restore 3-22

U

- Unix
 - qtrees 2-7



CommVault® Systems, Inc.

2 Crescent Place

P.O. Box 900

Oceanport, NJ 07757-0900

Phone: (732) 870-4000

Web: www.commvault.com