Features - Media Management

TABLE OF CONTENTS

HARDWARE MAINTENANCE

MEDIA MANAGEMENT

ADMINISTRATION

TROUBLESHOOTING

TOOLS

USE CASES

Overview - Media Management

Media management involves interaction among the CommServe, MediaAgents, client programs, storage devices and media. The sections that follow describe these entities as it relates to media management.

THE COMMSERVE STORAGEMANAGER

The following media-related software modules reside on the CommServe:

- The `Bull Calypso Media & Library Manager`, a service that processes media-related communications between the CommServe and client programs.
- An IEEE-standards compliant media management engine. This software accesses the media management database and communicates with storage devices through `Bull Calypso Media Mount Manager` in the MediaAgent. (discussed below).

In addition, the CommServe maintains a database containing the CommServe and MediaAgent related information.

THE MEDIAAGENT

The primary task of the MediaAgent™ is to oversee the transfer of data between client programs and media. Each MediaAgent communicates locally to one or more storage units via some local bus (e.g. SCSI) adapter and includes the following software modules:

- The `Bull Calypso Media Mount Manager`, a service that routes requests for media operations from the CommServe to the media management engine.
- Library Controller manages the hardware operations of the media changer within a storage device (e.g., mounting, unmounting, importing, and exporting media). If the library is directly attached to a MediaAgent then there is one library controller per media changer. If the library is attached to multiple MediaAgents in a SAN environment, one or more Library Controllers associated with the MediaAgents can be configured to control the same media changer.

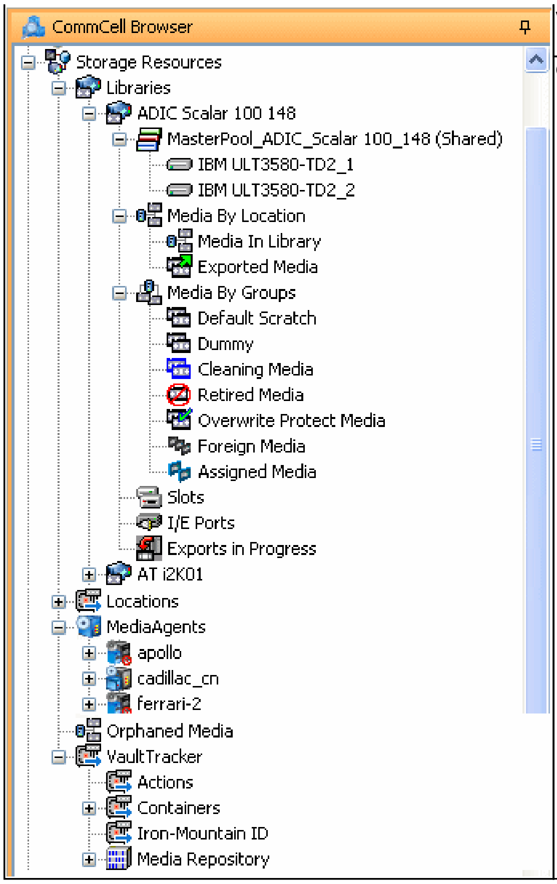
CLIENT PROGRAMS

In the context of media management, a client program is any software module that can request media-related information or operations. Client programs include software residing on the CommServe, MediaAgents, and Clients computers. In fact, most components in the software access the media management subsystem. Requests for media management can be initiated by a user or by an internal operation. When a client program needs media-related information or operations, it sends a request to the CommServe, which routes the request to other modules within the media management system, as necessary.

COMMCELL CONSOLE TREE LEVELS FOR MEDIA MANAGEMENT

In the CommCell Browser the Media Management information is available under Storage Resources. Each of the libraries configured in the library are displayed. The tree structure varies, depending on the library type - tape/optical library, stand-alone drive or disk libraries. This arrangement is reflected in the following sample tree structure in the CommCell Browser:

	MediaAgents: See MediaAgents.
	Libraries: Library Operations and Library Properties
	Master Drive Pools and Drive Pools: See Master Drive Pools and Drive Pools
	Drives: Drive Operations and Drive Properties
	Resource View: See Resource View.
	Media By Location: See Media By Location
	Media By Groups: See Media By Groups
	Disk Library and Mount Path: See Disk Libraries
	Stand-Alone Drives: See Stand-Alone Drives. (Removable Disk Drives are also displayed as stand-alone drives.)

<table>
<tr>
<td rowspan="2">


</td>
<td><b>Vault Tracker</b>: See Vault Tracker and VaultTracker Enterprise</td>
</tr>
<tr>
<td><b>Orphaned Media</b>: See Orphaned Media</td>
</tr>
</table>

Use CommCell Console Control Panel to establish advanced media management parameters.

Back to Top

System Requirements - MediaAgent

The following requirements are for the MediaAgent:

OPERATING SYSTEM		PROCESSOR
AIX	AIX 7.1	Power PC (Includes IBM System p)
	AIX 6.1 64-bit	RS/6000 43P Model 150 - 375 MHZ or higher; Dual Processors recommended
	AIX 5.3 64-bit with technology level 6 and runtime library xlC.rte 8.0.0.0 or higher	RS/6000 43P Model 150 - 375 MHZ or higher; Dual Processors recommended
	AIX 5.3 32-bit with technology level 6 and runtime library xlC.rte 8.0.0.0 or higher Note that all AIX platforms support Logical Partitions (LPAR).	RS/6000 43P Model 150 - 375 MHZ or higher; Dual Processors recommended
HP-UX	HP-UX 11i v3 (11.31) 64-bit	Itanium
	HP-UX 11i v3 (11.31) 64-bit	HP-UX -PA RISC 300 MHZ or higher; Dual Processors recommended
	HP-UX 11i v2 (11.23) 64-bit	HP-UX -PA RISC 300 MHZ or higher; Dual Processors recommended
	HP-UX 11i v2 (11.23) 64-bit	Itanium
	HP-UX 11i v1 (11.11) 64-bit with a minimum of OS patch level of December 2008 patch bundle or higher (contact Hewlett Packard to obtain the patch)	HP-UX -PA RISC 300 MHZ or higher; Dual Processors recommended
	HP-UX 11i v1 (11.11) 32-bit with a minimum of OS patch level of December 2008 patch bundle or higher (contact Hewlett Packard to obtain the patch)	HP-UX -PA RISC 300 MHZ or higher; Dual Processors recommended
LINUX	**ORACLE LINUX**	
	Oracle Linux 5.x with glibc 2.5.x	Intel Pentium, x64 or compatible processors
	RED FLAG LINUX	
	Red Flag Linux AS 4.1 32-bit with glibc 2.3.x	Intel Pentium or compatible 650 MHz processor minimum recommended; Dual 1 GHz or higher processors recommended
	RED HAT ENTERPRISE LINUX AS/ES	
	Red Hat Linux AS 4.0 with glibc 2.3.x	Power PC (Includes IBM System p)
	Red Hat Enterprise Linux AS/ES 4.0 with glibc 2.3.x	Intel Pentium or compatible 650 MHz processor minimum recommended; Dual 1 GHz or higher processors recommended
	Red Hat Enterprise Linux AS/ES 4.0 with glibc 2.3.x	Itanium
	Red Hat Enterprise Linux AS/ES 4.0 with glibc 2.3.x	x64
	Red Hat Enterprise Linux AS 5.x with glibc 2.5	x64
	RED HAT ENTERPRISE LINUX/CENTOS	
	Red Hat Enterprise Linux/CentOS Server 5 with glibc 2.5.x	Power PC (Includes IBM System p)
	Red Hat Enterprise Linux/CentOS 6.x with glibc 2.12.x	Intel Pentium, Itanium, x64, Power PC (Includes IBM System p) or compatible processors
	Red Hat Enterprise Linux/CentOS 5.x with glibc 2.5.x	Intel Pentium, Itanium, x64, Power PC (Includes IBM System p) or compatible processors
	Red Hat Enterprise Linux/CentOS 5 Advanced Platform with glibc 2.5.x	Intel Pentium or compatible 650 MHz processor minimum recommended; Dual 1 GHz or higher processors recommended
	Red Hat Enterprise Linux/CentOS 5 Advanced Platform with glibc 2.5.x	Itanium, x64 or compatible processors
	SUSE LINUX (SLES)	
	SuSE Linux 11.x with glibc 2.9.x and above	x64
	SuSE Linux 11.x with glibc 2.9.x and above	Power PC (Includes IBM System p)

	SuSE Linux 11.x with glibc 2.9.x and above	Itanium
	SuSE Linux 11.x with glibc 2.9.x and above	Intel Pentium or compatible 650 MHz processor minimum recommended; Dual 1 GHz or higher processors recommended
	SuSE Linux 11.x with glibc 2.11.x	Intel Pentium, x64 or compatible processors
	SuSE Linux 10 Enterprise Server Edition with glibc 2.4.x	Intel Pentium or compatible 650 MHz processor minimum recommended; Dual 1 GHz or higher processors recommended
	SuSE Linux 10 Enterprise Server Edition with glibc 2.4.x	Itanium
	SuSE Linux 10 Enterprise Server Edition with glibc 2.4.x	Power PC (Includes IBM System p)
	SuSE Linux 10 Enterprise Server Edition with glibc 2.4.x	x64
	UBUNTU	
	Ubuntu 10.04 LTS	Intel Pentium, x64 or compatible processors
SOLARIS	Solaris 9 4/04 64-bit	Ultra5 station or higher; Dual Processors recommended
	Solaris 9 4/04 32-bit	Ultra5 station or higher; Dual Processors recommended
	Solaris 11.x	x64
	Solaris 11.x	Ultra5 station or higher; Dual Processors recommended
	Solaris 10.x with a minimum of SunOS (Sparc) Patch 119963-14	Ultra5 station or higher; Dual Processors recommended
	Solaris 10.x 64-bit	x64
TRU64	Tru64 OSF1 Release 5.1B-3	CompaqÂ® (DEC) AlphaServer DS Series computer or higher recommended
WINDOWS	**WINDOWS 2012**	
	Microsoft Windows Server 2012 Editions See Considerations for Microsoft Windows Server 2012, 2012 R2, and Windows 8 for more information.	All Windows-compatible processors supported
	WINDOWS 8	
	Microsoft Windows 8 Editions* *Tape Libraries/Drives are not supported. See Considerations for Microsoft Windows Server 2012, 2012 R2, and Windows 8 for more information.	All Windows-compatible processors supported
	WINDOWS 7	
	Microsoft Windows 7 Editions* *Tape Libraries/Drives are not supported.	All Windows-compatible processors supported
	WINDOWS 2008	
	Microsoft Windows Server 2008 32-bit and x64 Editions* *Web Server Editions not supported	All Windows-compatible processors supported
	WINDOWS VISTA	
	Microsoft Windows Vista Editions* *Tape Libraries/Drives are not supported.	All Windows-compatible processors supported
	WINDOWS 2003	
	Microsoft Windows Server 2003 32-bit, 64-bit and x64 Editions* with a minimum of Service Pack 1	All Windows-compatible processors supported
	Microsoft Windows Server 2003 32-bit Editions** with a minimum of Service Pack 1 (as guest OS/virtual machine) on VMware GSX and ESX **On VMware virtual machines, Hyper-V virtual machines, and Hyper-V R2 Core machines, Disk Library configuration is supported.	All Windows-compatible processors supported
	WINDOWS XP	
	Microsoft Windows XP Editions* with a minimum of Service Pack 3	All Windows-compatible processors supported

*Tape Libraries/Drives are not supported.

HARD DRIVE

WINDOWS

130 MB for the MediaAgent software and log file growth/ 298 MB recommended

Enough additional local disk space to accommodate the index cache (with a minimum of 256 MB). It is recommended that the index cache is configured to be written on a partitioned drive, used exclusively for holding index cache. For information on calculating the space requirements for index cache, see Calculating the Storage Space Required for the Index Cache Directory.

> An undersized index cache can result in degraded backup and restore performance. A severely undersized index cache can render backups and restores on that MediaAgent inoperable.

732 MB of free disk space on the drive in which the Operating System and `temp` directory resides, to copy temporary files during the install or upgrade process.

UNIX

256 MB for the MediaAgent software and log file growth

MEMORY

4 GB RAM minimum required; 32 GB RAM recommended if MediaAgent is used with Deduplication. For granular details on MediaAgent sizing, refer to the Deduplication Building Block Guide.

Virtual memory should be set to twice the amount of available physical memory.

A MediaAgent that is also a Catalog Server requires an additional hard disk space of 4% of the total data protected by all MediaAgents using the Catalog Server.

PERIPHERALS

DVD-ROM drive

SCSI bus adapter for each attached media library

Sufficient hard disk space when backing up to disk drives
Swap space = 2*RAM size

Media library or stand-alone drive attached to local SCSI adapter(s), backup device available through Storage Area Network (SAN), or magnetic disk partitions for backup data.

> Contact your software provider, for a list of supported storage devices (libraries, drives, media and SAN devices) and compatible SCSI cards.

MISCELLANEOUS

NETWORK

TCP/IP Services configured on the computer.

DRIVERS

Drivers for SCSI Adapters (Supplied by your SCSI Adapter provider)

Drivers for media drives (Supplied by your media drive provider)

.NET FRAMEWORK

.NET Framework 2.0 is automatically installed. Note that .NET Framework 2.0 can co-exist with other versions of this software.

MICROSOFT VISUAL C++

Microsoft Visual C++ 2008 Redistributable Package is automatically installed. Note that Visual C++ 2008 Redistributable Package can co-exist with other versions of this software.

SELINUX

If you have SELinux enabled on the client computer, create the SELinux policy module as a root user before performing a backup. The SELinux Development package must be installed on the client.

To create an SELinux policy module, perform the following steps as user "root":

1. Create the following files in the /usr/share/selinux/devel directory:

File Name	Content of the File
<directory>/<file_name>.te where: <directory> is /usr/share/selinux/devel <file_name> is the name of the Unix file, created to save the policy module statement. It is a good idea to use the same name for policy module and the file. For example: When you are creating a policy module for backup_IDA application, you can use the following file name: backup_IDA.te	The content of the file should be as follows: policy_module(<name>,<version>) ############################## where: <name> is the name of the policy module. You can give any unique name to the policy module, such as a process or application name. <version> is the version of the policy module. It can be any number, such as 1.0.0. For Example: While creating a policy module for the backup_IDA application, you can use the following content. policy_module(backup_IDA,1.0.0)
<directory>/<file_name>.fc where: <directory> is /usr/share/selinux/devel <file_name> is the name of the Unix file, created to save the policy module statement. It is a good idea to use the same name for policy module and the file. For example: When you are creating a policy module for backup_IDA application, you can use the following file name: backup_IDA.fc	The content of the file should be as follows: Note that the following list of files is not exhaustive. If the process fails to launch, check /var/log/messages. Also, if required, add it to the following list of files. /opt/<software installation directory>/Base/libCTreeWrapper.so -- gen_context (system_u:object_r:texrel_shlib_t,s0) /opt/<software installation directory>/Base/libCVMAGuiImplgso -- gen_context (system_u:object_r:texrel_shlib_t,s0) /opt/<software installation directory>/Base/libdb2locale.so.1 -- gen_context (system_u:object_r:texrel_shlib_t,s0) /opt/<software installation directory>/Base/libdb2osse.so.1 -- gen_context (system_u:object_r:texrel_shlib_t,s0) /opt/<software installation directory>/Base/libDb2Sbt.so -- gen_context (system_u:object_r:texrel_shlib_t,s0) /opt/<software installation directory>/Base/libdb2trcapi.so.1 -- gen_context (system_u:object_r:texrel_shlib_t,s0) /opt/<software installation directory>/Base/libDrDatabase.so -- gen_context (system_u:object_r:texrel_shlib_t,s0) /opt/<software installation directory>/Base/libIndexing.so -- gen_context (system_u:object_r:texrel_shlib_t,s0) /opt/<software installation directory>/Base/libSnooper.so -- gen_context (system_u:object_r:texrel_shlib_t,s0)

2. Create the policy file from command line. Use the following command. Ensure that you give the following commands in the /usr/share/selinux/devel directory.

```
[root]# make backup_IDA.pp
Compiling targeted backup_IDA module
/usr/bin/checkmodule: loading policy configuration from tmp/backup_IDA.tmp
/usr/bin/checkmodule: policy configuration loaded
/usr/bin/checkmodule: writing binary representation (version 6) to tmp/backup_IDA.mod
Creating targeted backup_IDA.pp policy package
rm tmp/backup_IDA.mod tmp/backup_IDA.mod.fc
[root]# semodule -i backup_IDA.pp
[root]#
```

3. Execute the policy module. Use the following command:

```
[root]# restorecon -R /opt/<software installation directory>
```

SELinux is now configured to work with this application.

NOTES ON MEDIAAGENT INSTALLATION

The MediaAgent should not be installed on a compressed drive.

On Unix 64-bit computers, you can opt to install either the 32-bit version or 64-bit version of the agent. See Install the MediaAgent or Linux File System Deployment to run the appropriate install.

For information on installing the MediaAgent software on the Microsoft Virtual Server, see Considerations for backing up the Microsoft Virtual Server.

(If CommServe, MediaAgent and Client software are installed on the same computer.)

Contact your software provider, for a list of supported storage devices (libraries, drives, media and SAN devices) and compatible SCSI cards.

DISCLAIMER

Minor revisions and/or service packs that are released by application and operating system vendors are supported by our software but may not be individually listed in our System Requirements. We will provide information on any known caveat for the revisions and/or service packs. In some cases, these revisions and/or service packs affect the working of our software. Changes to the behavior of our software resulting from an application or operating system revision/service pack may be beyond our control. The older releases of our software may not support the platforms supported in the current release. However, we will make every effort to correct the behavior in the current or future releases when necessary. Please contact your Software Provider for any problem with a specific application or operating system.

Additional considerations regarding minimum requirements and End of Life policies from application and operating system vendors are also applicable

Install the MediaAgent - Windows

TABLE OF CONTENTS

INSTALL REQUIREMENTS

The following procedure describes the steps involved in installing the Windows MediaAgent on both clustered and non-clustered environment. The Windows MediaAgent is installed on a computer that satisfies the minimum requirements specified in System Requirements - MediaAgent.

Review the following Install Requirements before installing the software:

GENERAL

- The MediaAgent can only be installed after the CommServe® software has already been installed. Also, keep in mind that the CommServe® software must be running (but not necessarily on the same computer) before you can install the MediaAgent.
- This version of the software is intended to be installed where the CommServe Server is in 9.0.0.
- Ensure that you have an available license on the CommServe for the MediaAgent. Also, if you wish to install the NDMP Remote Server, make sure that you have an appropriate license.
- Do not install the MediaAgent on a compressed drive.
- Close all applications and disable any programs that run automatically, including anti-virus, screen savers and operating system utilities. Some of the programs, including many anti-virus programs, may be running as a service. Stop and disable such services before you begin. You can re-enable them after the installation.
- Ensure the account under which the **Bull Calypso Communications Service (GxCVD)** runs has Full permissions to all files and folders on drives where backups will occur. By default the *i*DataAgent uses the System account, which should have access to all objects on the client.
- Verify that you have the software installation disc that is appropriate to the destination computer's operating system.

  Make sure that you have the latest software installation disc before you start to install the software. If you are not sure, contact your software provider.

NETWORK

- If your MediaAgent computer has multiple Network Interface Cards and IP addresses, make certain that all network communication paths are working. Also, make sure that the network interface to be used in the MediaAgent installation is set as the first one to be bound on the network. For more information on Network Interface Cards, see Network Requirements.

CLUSTER SPECIFIC

- The MediaAgent can be installed from the active node in the cluster group using the following procedure. The software can also be automatically installed on all available passive nodes when the software is installed in the cluster group, or you can choose to install any passive node(s) separately.
- Check the following on the cluster computer in which you wish to install the software:
  - Cluster software is installed and running.
  - Active and passive nodes are available.
  - Disk array devices configured with access to the shared array.
  - Public Network Interface Card is bound first, before the private Network Interface Card. (Does not apply to NetWare Cluster.)

BEFORE YOU BEGIN

- Log on to the computer that will serve as the MediaAgent as a local `Administrator` or as a member of the `Administrators` group on that computer.
- On a clustered computer, ensure that you are logged on to the **active node** as the Domain User with administrative privileges to all nodes on the cluster.

INSTALL PROCEDURE

GETTING STARTED

1. Place the Software Installation Disc for the Windows platform into the disc drive.

   After a few seconds, the installation program is launched.

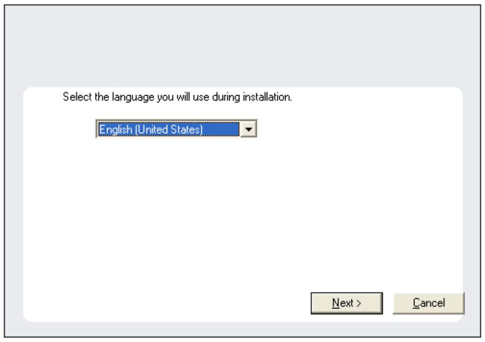
   If the installation program does not launch automatically:

   - Click the **Start** button on the Windows task bar, and then click **Run**.
   - Browse to the installation disc drive, select **Setup.exe**, click **Open**, then click **OK**.

   NOTES

   - If you are installing on Windows Server Core editions, mount to Software Installation Disc through command line, go to the **AMD64** folder and run **Setup.exe**.

2. Choose the language you want to use during installation. Click the down arrow and select the desired language from the drop-down list, and click **Next** to continue.



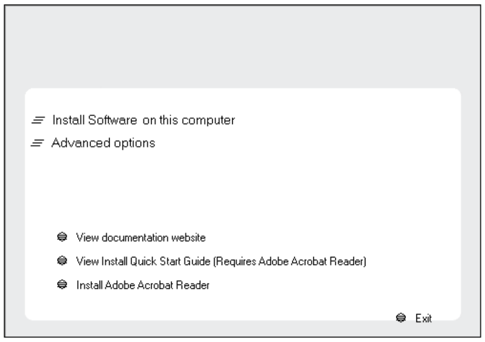
Select the language you will use during installation.

English (United States)

3. Select the option to install software on this computer.

   NOTES

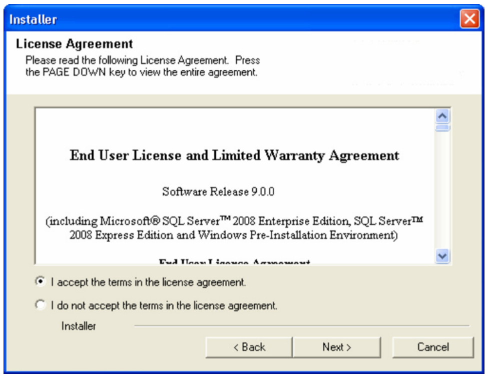
   - The options that appear on this screen depend on the computer in which the software is being installed.



Install Software on this computer
Advanced options
View documentation website
View Install Quick Start Guide (Requires Adobe Acrobat Reader)
Install Adobe Acrobat Reader
Exit

4. Read the license agreement, then select **I accept the terms in the license agreement**.

   Click **Next** to continue.



Installer

License Agreement

Please read the following License Agreement. Press the PAGE DOWN key to view the entire agreement.

End User License and Limited Warranty Agreement

Software Release 9.0.0

(including Microsoft® SQL Server™ 2008 Enterprise Edition, SQL Server™ 2008 Express Edition and Windows Pre-Installation Environment)

● I accept the terms in the license agreement.

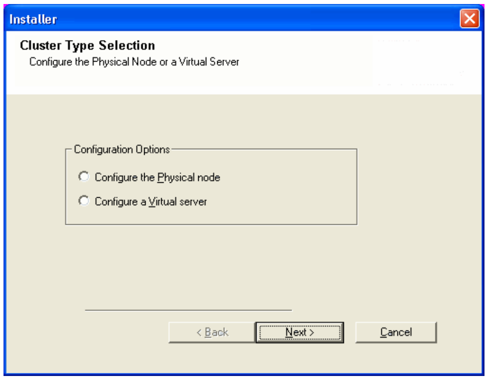
○ I do not accept the terms in the license agreement.

CLUSTER SELECTION

If you are installing in clustered environment, follow the steps below. For non-clustered environment, skip to Select Components for Installation.

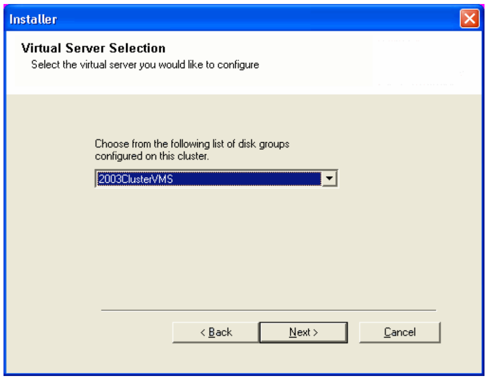
5. Select **Configure a Virtual Server**.

   Click **Next** to continue.


Installer
Cluster Type Selection
Configure the Physical Node or a Virtual Server
Configuration Options
○ Configure the Physical node
○ Configure a Virtual server
< Back
Next >
Cancel

6. Select the disk group in which the cluster group resides.

Click **Next** to continue.



Choose from the following list of disk groups configured on this cluster.

2003ClusterVMS

SELECT COMPONENTS FOR INSTALLATION

7. Select the component(s) to install.

NOTES

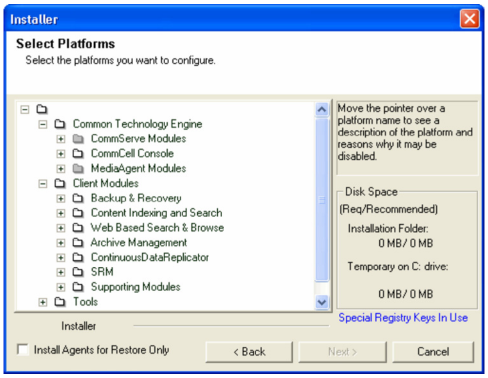
- Your screen may look different from the example shown.
- Components that either have already been installed, or which cannot be installed, will be dimmed. Hover over the component for additional details.
- If you wish to install the agent software for restore only, select **Install Agents for Restore Only** checkbox. See Installing Restore Only Agents for more information.
- The **Special Registry Keys In Use** field will be highlighted when `GalaxyInstallerFlags` registry key is enabled. Move the mouse pointer over this field to see a list of registry keys that have been created in this computer.

Click **Next** to continue.

To install the MediaAgent, under `Common Technology Engine` expand the `MediaAgent Modules` and select `MediaAgent`.

Optionally you can also select the following MediaAgent components at this time:

- `NDMP Remote Server` - Select this option if your MediaAgent has a library attached and is used by a NAS NDMP client to backup data. (Requires that you have an appropriate license on the CommServe.)



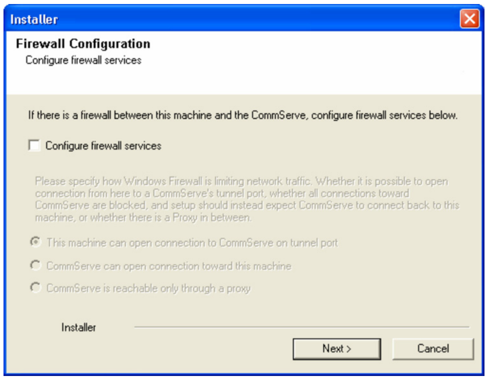
Move the pointer over a platform name to see a description of the platform and reasons why it may be disabled.

CONFIGURATION OF OTHER INSTALLATION OPTIONS

8. If this computer and the CommServe is separated by a firewall, select the **Configure firewall services** option and then click **Next** to continue.

For firewall options and configuration instructions, see Firewall Configuration and continue with the installation.

If firewall configuration is not required, click **Next** to continue.



Firewall Configuration
Configure firewall services

If there is a firewall between this machine and the CommServe, configure firewall services below.

□ Configure firewall services

Please specify how Windows Firewall is limiting network traffic. Whether it is possible to open connection from here to a CommServe's tunnel port, whether all connections toward CommServe are blocked, and setup should instead expect CommServe to connect back to this machine, or whether there is a Proxy in between.

● This machine can open connection to CommServe on tunnel port

○ CommServe can open connection toward this machine

○ CommServe is reachable only through a proxy

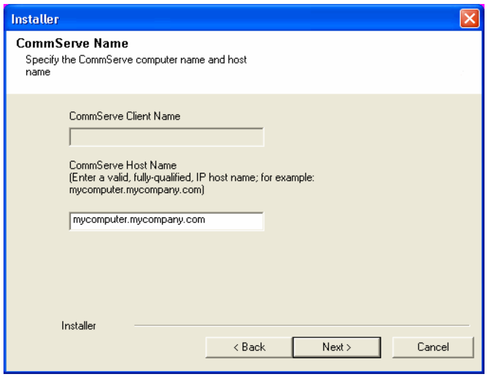
9. Enter the fully qualified domain name of the CommServe Host Name. This should be TCP/IP network name. e.g., computer.company.com.

NOTES

- The CommServe client name is the name of the computer. This field is automatically populated.
- Do not use space and the following characters when specifying a new name for the CommServe Host Name:

  \|`~!@#$%^&*()+=<>/?,[]{}:;'"
- If a computer has already been installed, this screen will not be displayed; instead the installer will use the same Server Name as previously specified.
- If you do not specify the CommServe Host Name, a window will be prompted to continue in decouple mode. Click **Yes** to continue to Decoupled Install. Click **No** to specify a CommServe Name and continue with the installation.

Click **Next** to continue.



CommServe Name
Specify the CommServe computer name and host name

CommServe Client Name

CommServe Host Name
(Enter a valid, fully-qualified, IP host name; for example: mycomputer.mycompany.com)

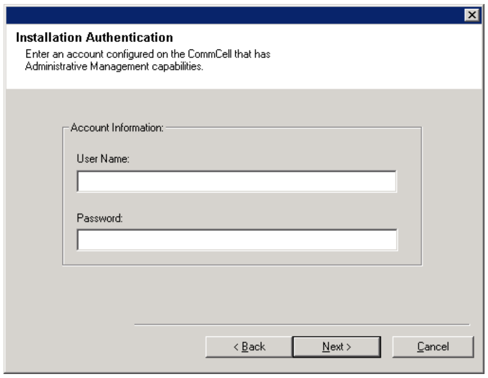
mycomputer.mycompany.com

10. Enter the **username** and **password** associated with an external domain user account or a CommCell user account to authorize the installation of this agent.

NOTES

- This window will be displayed when the **Require Authentication for Agent Installation** option is selected in the **CommCell Properties**. For more information, see Authentication for Agent Installs.

Click **Next** to continue.



Installation Authentication
Enter an account configured on the CommCell that has Administrative Management capabilities.

Account Information:

User Name:

Password:

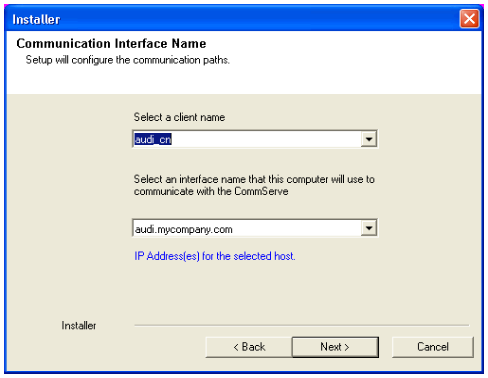
11. Enter the following:

- The local (NetBIOS) name of the client computer.
- The TCP/IP IP host name of the NIC that the client computer must use to communicate with the CommServe Server.

NOTES

- Do not use spaces when specifying a new name for the Client.
- The default network interface name of the client computer is displayed if the computer has only one network interface. If the computer has multiple network interfaces, enter the interface name that is preferred for communication with the CommServe Server.
- If a component has already been installed, this screen will not be displayed; instead, the install program will use the same name as previously specified.

Click **Next** to continue.



Communication Interface Name
Setup will configure the communication paths.

Select a client name

audi_cn

Select an interface name that this computer will use to communicate with the CommServe

audi.mycompany.com

IP Address(es) for the selected host.

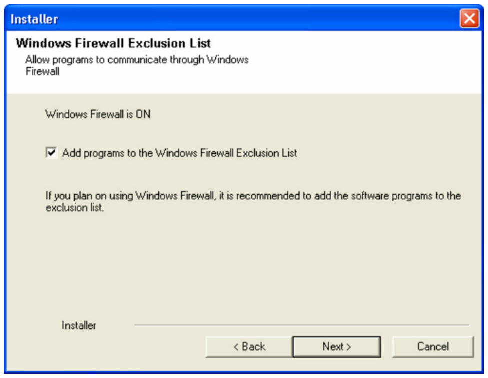
12. Select **Add programs to the Windows Firewall Exclusion List**, if you wish to add CommCell programs and services to the Windows Firewall Exclusion List.

NOTES:

- If Windows Firewall is enabled on the computer, this option is selected by default and must be enabled to proceed with the installation.
- If Windows Firewall is disabled on the computer, you can select this option to add the programs and services to enabled CommCell operations across the firewall, if the firewall is enabled at a later time.

You can either select this option during install or add the programs and services after installation. For adding the programs and services after installation, see Configure Windows Firewall to Allow CommCell Communication.

Click **Next** to continue.



Installer

Windows Firewall Exclusion List

Allow programs to communicate through Windows Firewall

Windows Firewall is ON

☑ Add programs to the Windows Firewall Exclusion List

If you plan on using Windows Firewall, it is recommended to add the software programs to the exclusion list.

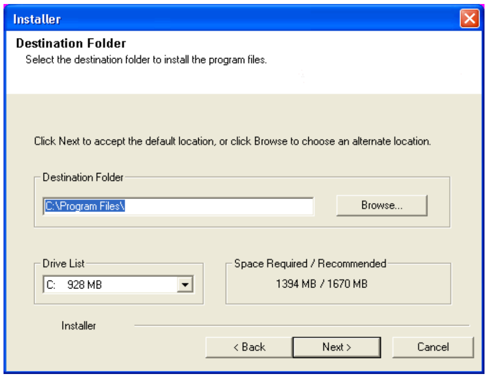
13. Specify the location where you want to install the software.

NOTES

- Do not install the software to a mapped network drive.
- Do not use the following characters when specifying the destination path:
  / : * ? " < > | #
  It is recommended that you use alphanumeric characters only.
- If you intend to install other components on this computer, the selected installation directory will be automatically used for that software as well.
- If a component is already installed in this computer, this screen may not be displayed. The software will be automatically installed in the same location that was previously specified.

Click **Browse** to change directories.

Click **Next** to continue.



Installer

Destination Folder

Select the destination folder to install the program files.

Click Next to accept the default location, or click Browse to choose an alternate location.

Destination Folder: C:\Program Files\

Drive List: C: 928 MB

Space Required / Recommended: 1394 MB / 1670 MB

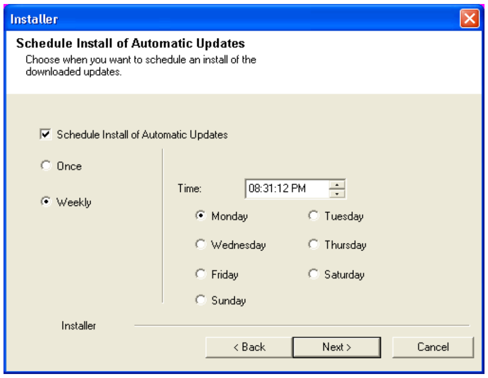
SCHEDULE AUTOMATIC UPDATE

14. If necessary, select this option to schedule an automatic installation of software updates.

NOTES

- Schedule Install of Automatic Updates allows automatic installation of the necessary software updates on the computer on a single or weekly basis. If you do not select this option, you can schedule these updates later from the CommCell Console.
- To avoid conflict, do not schedule the automatic installation of software updates to occur at the same time as the automatic FTP downloading of software updates.
- If a component has already been installed, this screen will not be displayed; instead, the installer will use the same option as previously specified.

Click **Next** to continue.



Installer

Schedule Install of Automatic Updates

Choose when you want to schedule an install of the downloaded updates.

☑ Schedule Install of Automatic Updates

○ Once

● Weekly

Time: 08:31:12 PM

● Monday ○ Tuesday

○ Wednesday ○ Thursday

○ Friday ○ Saturday

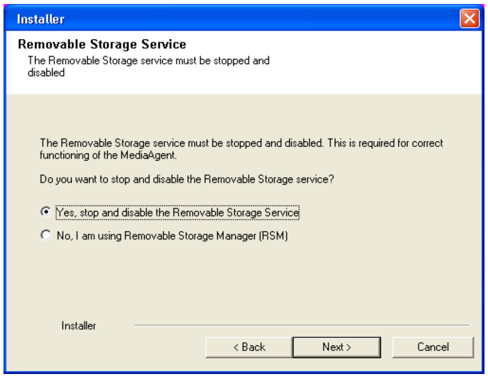
○ Sunday

15. Select **Yes** to stop Removable Storage Services on the MediaAgent.

NOTES

- This prompt will not appear if Removable Storage Services are already disabled on the computer.

Click **Next** to continue.



Installer

Removable Storage Service

The Removable Storage service must be stopped and disabled

The Removable Storage service must be stopped and disabled. This is required for correct functioning of the MediaAgent.

Do you want to stop and disable the Removable Storage service?

● Yes, stop and disable the Removable Storage Service

○ No, I am using Removable Storage Manager (RSM)

VERIFY SUMMARY OF INSTALL OPTIONS

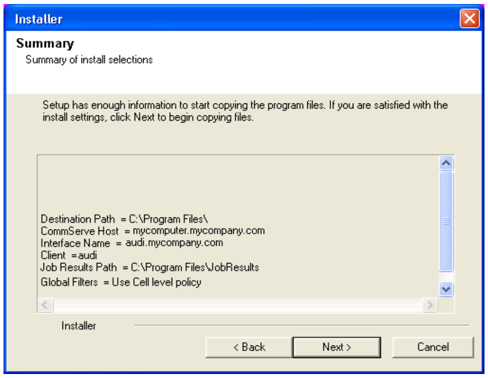
16. Verify the summary of selected options.

NOTES

- The **Summary** on your screen should reflect the components you selected for install, and may look different from the example shown.

Click **Next** to continue or **Back** to change any of the options.

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



Setup has enough information to start copying the program files. If you are satisfied with the install settings, click Next to begin copying files.

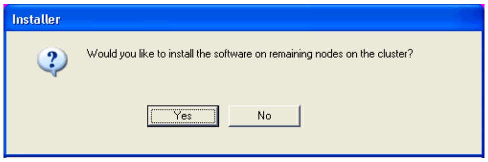
```
Destination Path  = C:\Program Files\
CommServe Host  = mycomputer.mycompany.com
Interface Name  = audi.mycompany.com
Client  =audi
Job Results Path  = C:\Program Files\JobResults
Global Filters  = Use Cell level policy
```

INSTALL REMAINING CLUSTER NODES

If you are installing in clustered environment, follow the steps below to install on remaining nodes of the cluster. For non-clustered environment, skip to Setup Complete.

17. To install/upgrade the software on the remaining nodes of the cluster, click **Yes**.

To complete the install for this node only, click **No**.



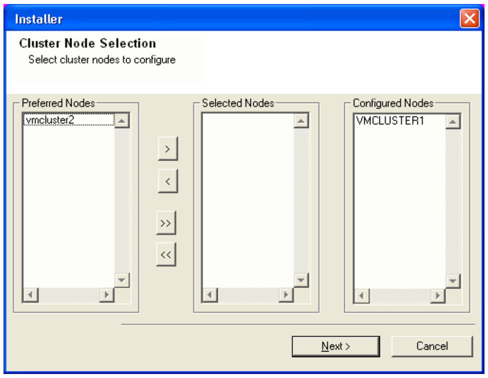
Would you like to install the software on remaining nodes on the cluster?

18. Select cluster nodes from the **Preferred Nodes** list and click the arrow button to move them to the **Selected Nodes** list.

NOTES

- The list of **Preferred Nodes** displays all the nodes found in the cluster; from this list you should only select cluster nodes configured to host this cluster group server.
- Do not select nodes that already have multiple instances installed. For more information, see Multi Instancing.

When you have completed your selections, click **Next** to continue.



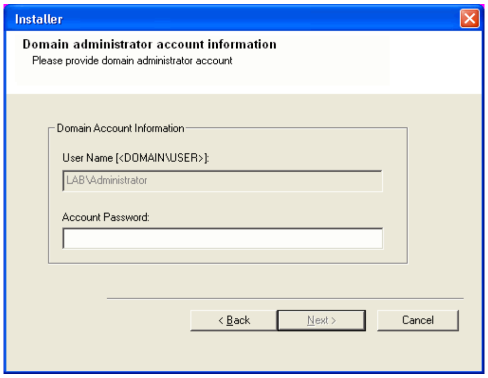
Preferred Nodes: vmcluster2

Selected Nodes:

Configured Nodes: VMCLUSTER1

19. Type the **User Name** and **Password** for the Domain Administrator account, so that the installer can perform the remote install/upgrade of the cluster nodes you selected in the previous step.

Click **Next** to continue.


Installer
Domain administrator account information
Please provide domain administrator account
Domain Account Information

User Name [<DOMAIN\USER>]: LAB\Administrator

Account Password:

20. The progress of the remote install for the cluster nodes is displayed; the install can be interrupted if necessary.

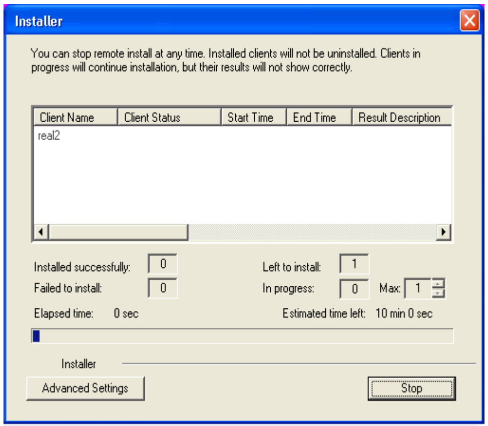
Click **Stop** to prevent installation to any nodes after the current ones complete.

Click **Advanced Settings** to specify any of the following:

- Maximum number of nodes on which Setup can run simultaneously.
- Time allocated for Setup to begin executing on each node, after which the install attempt will fail.
- Time allocated for Setup to complete on each node, after which the install attempt will fail.

NOTES

- If, during the remote install of a cluster node, setup fails to complete or is interrupted, you must perform a local install on that node. When you do, the install begins from where it left off, or from the beginning if necessary. For procedures, see Manually Installing the Software on a Passive Node.



Installer

You can stop remote install at any time. Installed clients will not be uninstalled. Clients in progress will continue installation, but their results will not show correctly.

Client Name	Client Status	Start Time	End Time	Result Description
real2				

Installed successfully: 0

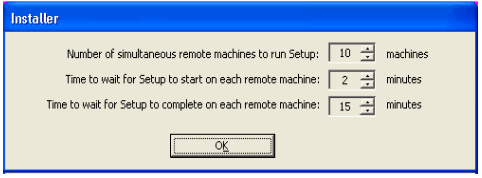
Failed to install: 0

Left to install: 1

In progress: 0 Max: 1

Elapsed time: 0 sec

Estimated time left: 10 min 0 sec



Installer

Number of simultaneous remote machines to run Setup: 10 machines

Time to wait for Setup to start on each remote machine: 2 minutes

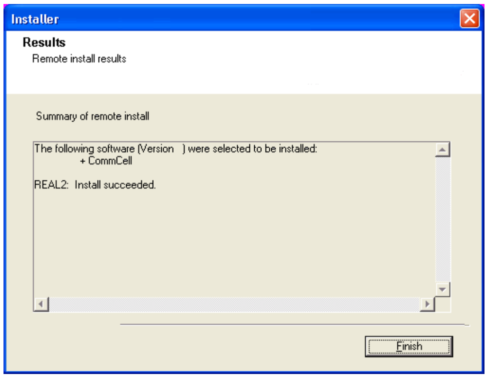
Time to wait for Setup to complete on each remote machine: 15 minutes

21. Read the summary for remote installation to verify that all selected nodes were installed successfully.

NOTES

- If any node installation fails, you must manually install the software on that node once the current installation is complete. (See Manually Installing the Software on a Passive Node for step-by-step instructions.)
- The message displayed on your screen will reflect the status of the selected nodes, and may look different from the example.

Click **Next** to continue.



Installer

Results

Remote install results

Summary of remote install

The following software (Version) were selected to be installed:
+ CommCell

REAL2: Install succeeded.

SETUP COMPLETE

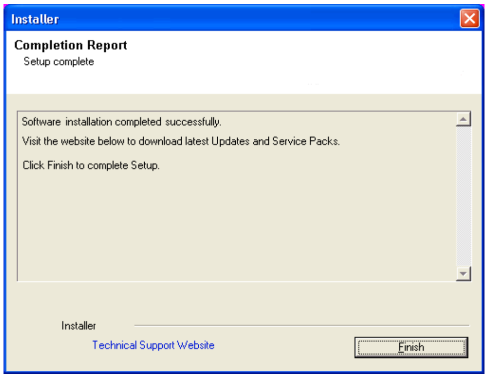
22. Setup displays the successfully installed components.

NOTES

- The **Setup Complete** message displayed on your screen will reflect the components you installed, and may look different from the example shown.
- If you install an Agent with the CommCell Console open, you need to refresh the CommCell Console (F5) to see the new Agents.
- If **Reboot Now** button is displayed make sure to reboot the computer before performing any other operations from the computer.

Click **Finish** to close the install program.

The installation is now complete.



Installer

Completion Report

Setup complete

Software installation completed successfully.

Visit the website below to download latest Updates and Service Packs.

Click Finish to complete Setup.

POST-INSTALL CONSIDERATIONS

GENERAL

- Review Install Considerations after installing the software.
- Install post-release updates or Service Packs that may have been released after the release of the software. When you are installing a Service Pack, ensure that it is the same version as the one installed in the CommServe Server. Alternatively, you can enable Automatic Updates for quick and easy installation of updates in the CommCell component.

Install the MediaAgent - Solaris

TABLE OF CONTENTS

INSTALL REQUIREMENTS

The following procedure describes the steps involved in installing the MediaAgent software on a Solaris computer. The MediaAgent can be installed on a computer that satisfies the minimum requirements specified in System Requirements - MediaAgent.

Review the following Install Requirements before installing the software:

GENERAL

- Review Install Considerations before installing the software.
- The MediaAgent can only be installed after the CommServe has already been installed in the CommCell. Also, keep in mind that the CommServe must be running before you can install the MediaAgent.
- This version of the software is intended to be installed in a CommCell with the latest version of CommServe.
- Ensure that you have an available license on the CommServe for the MediaAgent.
- Verify that you have the software installation disc that is appropriate to the destination computer's operating system.

  Make sure that you have the latest software installation disc before you start to install the software. If you are not sure, contact your software provider.

BEFORE YOU BEGIN

- Log on to the MediaAgent computer as `root`.
- The install package requires `super-user` permissions to execute.

INSTALL PROCEDURE

GETTING STARTED

1. Place the software installation disc for the Unix platform into the disc drive.

   You can also install the product using a disc drive mounted on another computer on the network.

   - On Solaris, double-click the **cvpkgadd** program from the File Manager window.
   - On other Unix platforms, open the Terminal window, navigate to the software installation disc and then enter **./cvpkgadd**.

2. The product banner and other information is displayed.

   Press **Enter** to continue.

3. Read the license agreement. Type **y** and press **Enter** to continue.

4. Enter the number corresponding to the setup task you want to perform.

   NOTES

   - For Install data protection agents on this computer option, follow the steps described in this procedure.
   - Advance options provide additional setup features such as record and play setup, creating a custom package and External Data Connector Agent software.

     To create a custom package and for record and play setup, follow the steps described in Custom Package - Unix.

     To install the External Data Connector Agent, follow the steps described in External Data Connector - Unix.

```
Please select a setup task you want to perform from the
list below:

Advance options provide extra setup features such as
creating custom package, recording/replaying user
selections and installing External Data Connector
software.

1) Install data protection agents on this computer

2) Advance options

3) Exit this menu

Your choice: [1]
```

5. If your computer is 32-bit, press **Enter**.

If your computer is 64-bit, see Install Unix Agents on 64-bit Platform for step-by-step procedure.

```
This machine supports both 32 bit and 64 bit binaries. By
default, we will install 32 bit binary set that has full
support for all the modules included in this package.
Please note that 64 bit binary set currently only support
limited modules.

1) All platforms (32 bit)

2) FS and MA only (64 bit)

Your choice: [1]
```

6. This prompt is displayed only when you are installing on AIX, HP-UX, Linux, or Solaris computers.

Press **Enter** to continue

NOTES

- When you install on non-clustered computer, you must select the number associated with the option **Install on a physical machine**.

```
Certain Calypso packages can be associated with a virtual
IP, or in other words, installed on a "virtual machine"
belonging to some cluster. At any given time the virtual
machine's services and IP address are active on only one
of the cluster's servers. The virtual machine can "fail-
over" from one server to another, which includes stopping
services and deactivating IP address on the first server
and activating the IP address/services on the other
server.

You now have a choice of performing a regular Calypso
install on the physical host or installing Calypso on a
virtual machine for operation within a cluster.

Most users should select "Install on a physical machine"
here.

1) Install on a physical machine

2) Install on a virtual machine

3) Exit

Your choice: [1]
```

7. If you have only one network interface, press **Enter** to accept the default network interface name and continue.

If you have multiple network interfaces, enter the number corresponding to the network interface that you wish to use as default, and then press **Enter** to continue.

NOTES

- The interface name and IP addresses depend on the computer in which the software is installed and may be different from the example shown.

```
We found one network interface available on your machine.
We will associate it with the physical machine being
installed, and it will also be used by the CommServe to
connect to the physical machine. Note that you will be
able to additionally customize Datapipe Interface Pairs
used for the backup data traffic later in the Calypso Java
GUI.

Please check the interface name below, and make
connections if necessary:

Physical Machine Host Name: [angel.company.com]
```

8. Specify the client name for the computer.

Press **Enter** to accept the default name and continue, or
Enter a new client name for the computer and then press **Enter** to continue.

```
Please specify the client name for this machine.

It does not have to be the network host name: you can
enter any word here without spaces. The only requirement
is that it must be unique on the CommServe.

Physical Machine Client name: [angel]
```

SELECT COMPONENTS FOR INSTALLATION

9. Enter the number corresponding to the **CVGxMA** module.

A confirmation screen will mark your choice with an "X". Type "d" for **Done**, and press **Enter** to continue.

NOTES

- To select multiple component, enter the number by adding a space.
- Your screen may look different from the example shown.
- Components that either have already been installed, or which cannot be installed, will not be shown.
- In addition, the list of modules that appear depends on the specific Unix File System in which the package is installed. (e.g., **CVGxWA** will appear only when the installation package is run on a Solaris computer.)

```
Install Calypso on physical machine client.company.com

Select the Calypso module that you would like to install

[ ] 1) Media Agent        [1301] [CVGxMA]
[ ] 2) FileSystem IDA     [1101] [CVGxIDA]
    >) >>>>> NEXT PAGE  >>>>>>

[a=all n=none r=reverse q=quit d=done >=next <=previous ?
=help]

Enter number(s)/one of "a,n,r,q,d,>,<,?" here: 2
```

BASE SOFTWARE INSTALLATION

10. If you wish to install the agent software for restore only, enter **Yes** and press **Enter** to continue. See Installing Restore Only Agents for more information.

Otherwise, accept **no**, press **Enter** to continue.

```
Do you want to use the agents for restore only without
consuming licenses? [no]
```

11. Type the appropriate number to install the latest software scripts and press **Enter** to continue.

NOTES

- Select **Download from the software provider website** to download the latest software scripts from your software provider website.

  Make sure you have internet connectivity when you are using this option.
- Select **Use the one in the installation media**, to install the software scripts

```
Installation Scripts Pack provides extra functions and
latest support and fix performed during setup time. Please
specify how you want to get this pack.

If you choose to download it from the website now, please
make sure you have internet connectivity at this time.
This process may take some time depending on the internet
connectivity.

1) Download from the software provider website.

2) Use the one in the installation media
```

from the disc or share from which the installation is performed.

- Select **Use the copy I already have by entering its unix path**, to specify the path if you have the software script in an alternate location.

```
3) Use the copy I already have by entering its unix path

Your choice: [1] 2
```

12. Enter **Yes** to download and install the latest service packs and post packs from the software provider.

NOTES

- Internet connectivity is required to download updates.
- This step is applicable for multi instancing.

Press **Enter** to continue.

```
Keep Your Install Up to Date - Latest Service Pack

Latest Service Pack provides extra functions and latest
support and fix for the packages you are going to install.
You can download the latest service pack from software
provider website.

If you decide to download it from the website now, please
make sure you have internet connectivity at this time.
This process may take some time depending on the internet
connectivity.

Do you want to download the latest service pack now? [no]

Press <ENTER> to continue ...
```

13. Specify the location where you want to install the software.

NOTES

- The amount of free space required depends on the components selected for install, and may look different from the example shown.

Press **Enter** to accept the default path and continue, or
Enter a path and then press **Enter** to continue.

Press **Enter** again to confirm the path.

```
Please specify where you want us to install Calypso
binaries.

It must be a local directory and there should be at least
98MB of free space available. All files will be installed
in a "calypso" subdirectory, so if you enter "/opt", the
files will actually be placed into "/opt/calypso".

Installation Directory: [/opt]

..

Calypso will be installed in /opt/calypso.
Press ENTER to continue ...
```

14. Specify the location for the log files.

NOTES

- All the modules installed on the computer will store the log files in this directory.
- The amount of free space required depends on the components selected for install, and may look different from the example shown.

Press **Enter** to accept the default path and continue, or
Enter a path and then press **Enter** to continue.

Press **Enter** again to confirm the path.

```
Please specify where you want to keep Calypso log files.

It must be a local directory and there should be at least
100MB of free space available. All log files will be
created in a "calypso/Log_Files" subdirectory, so if you
enter "/var/log", the logs will actually be placed into
"/var/log/calypso/Log_Files".

Log Directory: [/var/log]

..

Calypso log files will be created
in /var/log/calypso/Log_Files.
Press ENTER to continue ...
```

15. Indicate whether you would like to launch processes with inherent database access rights.

Press **Enter** to assign a new group, or
Type **No** and then press **Enter** to continue.

```
Most of Calypso processes run with root privileges, but
some are launched by databases and inherit database access
rights. To make sure that registry and log files can be
written to by both kinds of processes we can either make
such files world-writeable or we can grant write access
only to processes belonging to a particular group, e.g. a
"calypso" or a "dba" group.

We highly recommend now that you create a new user group
and enter its name in the next setup screen. If you choose
not to assign a dedicated group to Calypso processes, all
temporary and configuration files will be created with -
rw-rw-rw permissions.

If you're planning to backup Oracle DB you should use
"dba" group.

Would you like to assign a specific group to Calypso?
[yes]
```

16. If you indicated **Yes** in the previous step, you will be prompted for the group name that must be used to launch processes.

Enter the group name and then press **Enter** to continue.

Press **Enter** again to continue.

```
Please enter the name of the group which will be assigned
to all Calypso files and on behalf of which all Calypso
processes will run.

In most of the cases it's a good idea to create a
dedicated "calypso" group. However, if you're planning to
use Oracle iDataAgent or SAP Agent, you should enter
Oracle's "dba" group here.

Group name: dba

REMINDER

If you are planning to install Calypso Informix, DB2,
PostgreSQL, Sybase or Lotus Notes iDataAgent, please make
sure to include Informix, DB2, etc. users into group
"dba".
Press <ENTER> to continue ...
```

17. Type a network TCP port number for the Communications Service (CVD) and press **Enter**.

Type a network TCP port number for the Client Event Manager Service (EvMgrC) and press **Enter**.

NOTES

- For more information about Network TCP Ports, see Network TCP Port Requirements.
- For more information about these services, see Services.

```
Every instance of Calypso should use a unique set of
network ports to avoid interfering with other instances
running on the same machine.
The port numbers selected must be from the reserved port
number range and have not been registered by another
application on this machine.

Please enter the port numbers.

Port Number for CVD : [8600]

Port Number for EvMgrC: [8602]
```

- If the port number you entered already exists, a message will be displayed `Port #### is already reserved in /etc/services`. To work around this issue, enter different port number.

18. If this computer and the CommServe is separated by a firewall, type **Yes** and then press **Enter** to continue.

For firewall options and configuration instructions, see Firewall Configuration and continue with the installation.

If you do not wish to configure the firewall services, type **No** and then press **Enter** to continue.

```
Is there a firewall between this client and the CommServe?
[no]
```

19. Type the name of the CommServe computer and press **Enter** to continue.

NOTES

- Ensure that the CommServe is accessible before typing the name; otherwise the installation will fail.
- If you enter a short name which resolves to the same IP address as the fully qualified CommServe name, you will be asked if you would prefer to use the fully qualified name.

```
Please specify hostname of the CommServe below. Make sure
the hostname is fully qualified, resolvable by the name
services configured on this machine.

CommServe Host Name:
```

20. Enter the **username** and **password** information for an external domain user account or a CommCell user account. This authorizes the installation of an agent on the CommCell.

NOTES

- This is only displayed when the **Authentication for Agent** feature is enabled in the CommCell Properties. Users must belong to a User Group with Agent Management capabilities to enable this feature. For more information, see Authentication for Agent Installs.

Click **Enter** to continue.

```
Enter your CommCell user name and password:

User Name :

Password :

Press <ENTER> to continue ...
```

KERNEL PARAMETERS

21. Enter the appropriate number of streams, and then press **Enter** to continue, or Press **Enter** to accept the default number of streams and continue.

NOTES

- The number of streams specified ensures that concurrent backup/restore streams would have sufficient system resources. For more information on the subject, see Configuring Kernel Parameters for Macintosh and Configuring Kernel Parameters for Solaris.

This prompt is relevant only when you install/upgrade on a Macintosh or Solaris computer as appropriate.

```
Please enter the total number of streams that you plan to
run at the same time. We need to make sure that you have
enough semaphores and shared memory segments configured
in /etc/system.

Number of streams: [10]
```

22. Indicate whether you would like modifications to be made to the `/etc/system` configuration file.

Type **Yes**, and then press **Enter** to automatically update the file and continue, or Press **Enter** to accept the default **No** and continue (if you do not want to automatically update the file).

This prompt is displayed only when you install/upgrade on a Solaris (8 or 9) or Macintosh computer.

```
We now need to modify the /etc/system configuration file
on this computer. It is done to make sure that there will
be enough shared memory and semaphores available for
Calypso programs.

Please review the changes below and answer "yes" if you
want us to apply them to the /etc/system file. Otherwise,
the installation will proceed, the changes will be saved
to some other file, and you will have to apply them
manually.

set shmsys:shminfo_shmmni=8570 (was 7930)
set shmsys:shminfo_shmseg=8420 (was 7780)
set semsys:seminfo_semmns=10320 (was 9680)
set semsys:seminfo_semmni=8570 (was 7930)
set semsys:seminfo_semmsl=8570(was 7930)

Do you want us to apply these changes now? [no]

Changes saved into /etc/system.gal.1744

Press <ENTER> to continue.
```

23. If you indicated **No** in the previous step, the file to which the changes have been saved is displayed.
Make sure that these values are established later to ensure that all the requirements for this setup is satisfied.

NOTES

- The settings that are displayed are the maximum or minimum required settings. Value ’640’, which is provided for various shared memory segment or semaphore requirements, is a maximum value based on 10 streams.

Press **Enter** to continue.

This prompt is displayed only when you install/upgrade on a Solaris (8 or 9) computer, in cases where the install detects that the computer does not have the maximum or minimum required shared memory settings.

```
Although a ’no’ answer can be selected to this question
during install, the user should make sure the min
requirements (below) for shared memory are met, otherwise
the backups may fail (the message in logs is ’could not
start the pipeline’).

set shmsys:shminfo_shmmax=4199304
set shmsys:shminfo_shmmin=1
set semsys:shminfo_shmmni=640
set semsys:shminfo_shmseg=640
set semsys:seminfo_semmns=640
set semsys:seminfo_semmni=640
set semsys:seminfo_semmsl=640
set maxusers=256
```

CONFIGURE THE ACSLS LIBRARIES

24. Type **Yes** and then press **Enter** if you wish to configure StorageTek ACSLS libraries.

Press **Enter** if you do not wish to configure StorageTek ACSLS libraries.

```
Would you like to configure StorageTek ACSLS Enabled
Libraries on this MediaAgent?
Configure? [no]
```

25. Press **Enter** to accept the default host name and continue, or
Enter the name of the host in which the ACSLS server is installed and then press **Enter** to continue.

If you are accessing the library using SN6000, enter the host name of SN6000 and then press **Enter** to continue.

```
Please enter the name of the host running the ACSLS
daemon.
ACSLS Server host name:
```

26. The install program now starts copying the software to the computer. The progress of the operation is displayed.

```
.....
.....
.....
.....
Successfully copied xx files
```

CONFIGURE THE INDEX CACHE

27. Specify the location for the MediaAgent's Index Cache.

NOTES

- You can accept the default or choose another location. In either case, the location must be local.
- If desired, you can change the index cache location to a network drive from the CommCell Console, any time after you have installed the MediaAgent software.
- The recommended minimum space required for the index cache directory is 256 MB.
- It is recommended that the index cache location to be on a partitioned drive used exclusively for holding an index cache.
- For information on calculating the space requirements for index cache, see Calculating the Storage Space Required for Index Cache.
- Do not specify the root directory as the index cache directory.

Press **Enter** to accept the default path and continue, or
Enter a path and then press **Enter** to continue.

```
MediaAgent maintains a cache of indices for completed
backups. Normally they're stored
in /test1/calypso/MediaAgent/IndexCache directory, but you
can keep them anywhere. You can even make an IndexCache
directory shared by two or more MediaAgents.

Please specify where you want us to store the Index Cache.

Cache Directory:
```

28. Press **Enter** to continue.

NOTES

- This prompt is displayed when the specified Index Cache directory is not found.
If you wish to specify another directory for Index Cache, type **No** and then press **Enter**.
Specify the location for the MediaAgent's Index Cache.
- The index cache directory depends on the directory that you specified in the previous step and may appear different from the example shown.

```
Directory "/test1/calypso/MediaAgent/IndexCache" does not
exist.

Are you sure you entered its name correctly? [yes]
```

29. Press **Enter** to acknowledge the successful completion of the MediaAgent software installation.

```
Successfully installed CVGxMA.

Press ENTER to continue ...
```

CVGXWA INSTALLATION

In order for the Solaris MediaAgent to utilize a tape library attached to this computer, you must install the WA SCSI driver after installing the MediaAgent. If you are using only a disk library, it is not required to install the CVGxWA package.

If you do not want to install the WA SCSI driver, enter the number corresponding to **Exit** option and skip to Setup Complete.

30. The install program now starts copying the software to the computer. The progress of the operation is displayed.

Press **Enter** to continue.

```
.....
.....
.....
.....
Successfully copied xx files

.....
.....
Successfully installed <package_name>.

Press ENTER to continue ...
```

31. Type **Yes** and press **Enter** to load the WA driver into the kernel and create the device nodes without rebooting the system.

```
The loading of wa driver into the kernel may result in
scanning of attached devices on the system bus. This may
take some time. Please answer yes if you want to load
driver into the kernel now, otherwise we will do soft load
of the driver into kernel which may require a reboot.

Do you want us to load the driver into the kernel(yes/no)?
[yes]
```

SETUP COMPLETE

32. Enter the number corresponding to the **Exit** option and then press **Enter** to continue.

The installation is now complete.

```
Certain Calypso packages can be associated with a virtual
IP, or in other words, installed on a "virtual machine"
belonging to some cluster. At any given time the virtual
machine's services and IP address are active on only one
of the cluster's servers. The virtual machine can "fail-
over" from one server to another, which includes stopping
services and deactivating IP address on the first server
and activating the IP address/services on the other
server.

Currently you have Calypso installed on physical node
stone.company.com.

Now you have a choice of either adding another package to
the existing installation or configure Calypso on a
virtual machine for use in a cluster.

1) Add another package to stone.company.com
2) Install Calypso on a virtual machine
3) Exit

Your choice: [1]
```

POST-INSTALL CONSIDERATIONS

GENERAL

- Review Install Considerations after installing the software.
- Install post-release updates or Service Packs that may have been released after the release of the software. When you are installing a Service Pack, ensure that it is the same version as the one installed in the CommServe Server. Alternatively, you can enable Automatic Updates for quick and easy installation of updates in the CommCell component.

Install the MediaAgent - AIX, HP-UX, TRU64 or Linux

TABLE OF CONTENTS

INSTALL REQUIREMENTS

The following procedure describes the steps involved in installing the MediaAgent software on a Unix computer. The MediaAgent can be installed on a computer that satisfies the minimum requirements specified in System Requirements - MediaAgent.

Review the following Install Requirements before installing the software:

GENERAL

- Review Install Considerations before installing the software.
- The MediaAgent can only be installed after the CommServe has already been installed in the CommCell. Also, keep in mind that the CommServe must be running before you can install the MediaAgent.
- This version of the software is intended to be installed in a CommCell with the latest version of CommServe.
- Ensure that you have an available license on the CommServe for the MediaAgent.
- Verify that you have the software installation disc that is appropriate to the destination computer’s operating system.

  Make sure that you have the latest software installation disc before you start to install the software. If you are not sure, contact your software provider.

PACKAGE MANAGEMENT SYSTEMS

You can use the Red Hat Package Manager (RPM) package management system to install all Linux versions of the agent. Also, you can use the Advanced Packaging Tool (APT) package management system to install all Debian Linux versions of the agent. For step-by-step instructions, see Base Software Install for RPM Package Manager and Base Software Install for APT Package Manager.

RED HAT LINUX

Red Hat Linux will create an entry in the `/etc/hosts` file when it is first installed, in the following format:

<ip_address> <host name> `localhost`

For example, if the host name of your computer is `bluesky`, the entry will look something like this:

```
192.168.1.111 bluesky localhost
```

If you have not already done so, edit the `/etc/hosts` file. The edited entry should look like this:

```
127.0.0.1 localhost
```

Depending upon your environment, and using the above example again, you may also need an entry similar to this:

```
192.168.1.111 bluesky
```

BEFORE YOU BEGIN

- Log on to the MediaAgent computer as `root`.
- The install package requires `super-user` permissions to execute.

INSTALL PROCEDURE

GETTING STARTED

1. Place the software installation disc for the Unix platform into the disc drive.

   You can also install the product using a disc drive mounted on another computer on the network.

- On Solaris, double-click the **cvpkgadd** program from the File Manager window.
- On other Unix platforms, open the Terminal window, navigate to the software installation disc and then enter **./cvpkgadd**.

2. The product banner and other information is displayed.

Press **Enter** to continue.

3. Read the license agreement. Type **y** and press **Enter** to continue.

4. Enter the number corresponding to the setup task you want to perform.

NOTES

- For Install data protection agents on this computer option, follow the steps described in this procedure.
- Advance options provide additional setup features such as record and play setup, creating a custom package and External Data Connector Agent software.

  To create a custom package and for record and play setup, follow the steps described in Custom Package - Unix.

  To install the External Data Connector Agent, follow the steps described in External Data Connector - Unix.

```
Please select a setup task you want to perform from the
list below:

Advance options provide extra setup features such as
creating custom package, recording/replaying user
selections and installing External Data Connector
software.

1) Install data protection agents on this computer

2) Advance options

3) Exit this menu

Your choice: [1]
```

5. If your computer is 32-bit, press **Enter**.

If your computer is 64-bit, see Install Unix Agents on 64-bit Platform for step-by-step procedure.

```
This machine supports both 32 bit and 64 bit binaries. By
default, we will install 32 bit binary set that has full
support for all the modules included in this package.
Please note that 64 bit binary set currently only support
limited modules.

1) All platforms (32 bit)

2) FS and MA only (64 bit)

Your choice: [1]
```

6. This prompt is displayed only when you are installing on AIX, HP-UX, Linux, or Solaris computers.

Press **Enter** to continue

NOTES

- When you install on non-clustered computer, you must select the number associated with the option **Install on a physical machine**.

```
Certain Calypso packages can be associated with a virtual
IP, or in other words, installed on a "virtual machine"
belonging to some cluster. At any given time the virtual
machine's services and IP address are active on only one
of the cluster's servers. The virtual machine can "fail-
over" from one server to another, which includes stopping
services and deactivating IP address on the first server
and activating the IP address/services on the other
server.

You now have a choice of performing a regular Calypso
install on the physical host or installing Calypso on a
virtual machine for operation within a cluster.

Most users should select "Install on a physical machine"
here.

1) Install on a physical machine

2) Install on a virtual machine

3) Exit

Your choice: [1]
```

7. If you have only one network interface, press **Enter** to accept the default network interface name and continue.

If you have multiple network interfaces, enter the number corresponding to the network interface that you wish to use as default, and then press **Enter** to continue.

NOTES

- The interface name and IP addresses depend on the computer in which the software is installed and may be different from the example shown.

```
We found one network interface available on your machine.
We will associate it with the physical machine being
installed, and it will also be used by the CommServe to
connect to the physical machine. Note that you will be
able to additionally customize Datapipe Interface Pairs
used for the backup data traffic later in the Calypso Java
GUI.

Please check the interface name below, and make
connections if necessary:

Physical Machine Host Name: [angel.company.com]
```

8. Specify the client name for the computer.

Press **Enter** to accept the default name and continue, or
Enter a new client name for the computer and then press **Enter** to continue.

```
Please specify the client name for this machine.

It does not have to be the network host name: you can
enter any word here without spaces. The only requirement
is that it must be unique on the CommServe.

Physical Machine Client name: [angel]
```

SELECT COMPONENTS FOR INSTALLATION

9. Enter the number corresponding to the **CVGxMA** module.

A confirmation screen will mark your choice with an "X". Type "d" for **Done**, and press **Enter** to continue.

NOTES

- To select multiple component, enter the number by adding a space.
- Your screen may look different from the example shown.
- Components that either have already been installed, or which cannot be installed,

```
Install Calypso on physical machine client.company.com

Select the Calypso module that you would like to install

[ ] 1) Media Agent        [1301] [CVGxMA]
[ ] 2) FileSystem IDA     [1101] [CVGxIDA]
    >) >>>>> NEXT PAGE  >>>>>>

[a=all n=none r=reverse q=quit d=done >=next <=previous ?
=help]

Enter number(s)/one of "a,n,r,q,d,>,<,?" here: 2
```

will not be shown.

- In addition, the list of modules that appear depends on the specific Unix File System in which the package is installed. (e.g., **CVGxWA** will appear only when the installation package is run on a Solaris computer.)

BASE SOFTWARE INSTALLATION

10. If you wish to install the agent software for restore only, enter **Yes** and press **Enter** to continue. See Installing Restore Only Agents for more information.

Otherwise, accept **no**, press **Enter** to continue.

```
Do you want to use the agents for restore only without
consuming licenses? [no]
```

11. Type the appropriate number to install the latest software scripts and press **Enter** to continue.

NOTES

- Select **Download from the software provider website** to download the latest software scripts from your software provider website.

  Make sure you have internet connectivity when you are using this option.
- Select **Use the one in the installation media**, to install the software scripts from the disc or share from which the installation is performed.
- Select **Use the copy I already have by entering its unix path**, to specify the path if you have the software script in an alternate location.

```
Installation Scripts Pack provides extra functions and
latest support and fix performed during setup time. Please
specify how you want to get this pack.

If you choose to download it from the website now, please
make sure you have internet connectivity at this time.
This process may take some time depending on the internet
connectivity.

1) Download from the software provider website.

2) Use the one in the installation media

3) Use the copy I already have by entering its unix path

Your choice: [1] 2
```

12. Enter **Yes** to download and install the latest service packs and post packs from the software provider.

NOTES

- Internet connectivity is required to download updates.
- This step is applicable for multi instancing.

Press **Enter** to continue.

```
Keep Your Install Up to Date - Latest Service Pack

Latest Service Pack provides extra functions and latest
support and fix for the packages you are going to install.
You can download the latest service pack from software
provider website.

If you decide to download it from the website now, please
make sure you have internet connectivity at this time.
This process may take some time depending on the internet
connectivity.

Do you want to download the latest service pack now? [no]

Press <ENTER> to continue ...
```

13. Specify the location where you want to install the software.

NOTES

- The amount of free space required depends on the components selected for install, and may look different from the example shown.

Press **Enter** to accept the default path and continue, or
Enter a path and then press **Enter** to continue.

Press **Enter** again to confirm the path.

```
Please specify where you want us to install Calypso
binaries.

It must be a local directory and there should be at least
98MB of free space available. All files will be installed
in a "calypso" subdirectory, so if you enter "/opt", the
files will actually be placed into "/opt/calypso".

Installation Directory: [/opt]

..

Calypso will be installed in /opt/calypso.
Press ENTER to continue ...
```

14. Specify the location for the log files.

NOTES

- All the modules installed on the computer will store the log files in this directory.
- The amount of free space required depends on the components selected for install, and may look different from the example shown.

Press **Enter** to accept the default path and continue, or
Enter a path and then press **Enter** to continue.

Press **Enter** again to confirm the path.

```
Please specify where you want to keep Calypso log files.

It must be a local directory and there should be at least
100MB of free space available. All log files will be
created in a "calypso/Log_Files" subdirectory, so if you
enter "/var/log", the logs will actually be placed into
"/var/log/calypso/Log_Files".

Log Directory: [/var/log]

..

Calypso log files will be created
in /var/log/calypso/Log_Files.
Press ENTER to continue ...
```

15. Indicate whether you would like to launch processes with inherent database access rights.

Press **Enter** to assign a new group, or
Type **No** and then press **Enter** to continue.

```
Most of Calypso processes run with root privileges, but
some are launched by databases and inherit database access
rights. To make sure that registry and log files can be
written to by both kinds of processes we can either make
such files world-writeable or we can grant write access
only to processes belonging to a particular group, e.g. a
"calypso" or a "dba" group.

We highly recommend now that you create a new user group
and enter its name in the next setup screen. If you choose
not to assign a dedicated group to Calypso processes, all
temporary and configuration files will be created with -
rw-rw-rw permissions.

If you're planning to backup Oracle DB you should use
"dba" group.

Would you like to assign a specific group to Calypso?
[yes]
```

16. If you indicated **Yes** in the previous step, you will be prompted for the group name that must be used to launch processes.

```
Please enter the name of the group which will be assigned
to all Calypso files and on behalf of which all Calypso
processes will run.
```

Enter the group name and then press **Enter** to continue.

Press **Enter** again to continue.

```
In most of the cases it's a good idea to create a
dedicated "calypso" group. However, if you're planning to
use Oracle iDataAgent or SAP Agent, you should enter
Oracle's "dba" group here.

Group name: dba

REMINDER

If you are planning to install Calypso Informix, DB2,
PostgreSQL, Sybase or Lotus Notes iDataAgent, please make
sure to include Informix, DB2, etc. users into group
"dba".
Press <ENTER> to continue ...
```

17. Type a network TCP port number for the Communications Service (CVD) and press **Enter**.

Type a network TCP port number for the Client Event Manager Service (EvMgrC) and press **Enter**.

NOTES

- For more information about Network TCP Ports, see Network TCP Port Requirements.
- For more information about these services, see Services.
- If the port number you entered already exists, a message will be displayed `Port #### is already reserved in /etc/services`. To work around this issue, enter different port number.

```
Every instance of Calypso should use a unique set of
network ports to avoid interfering with other instances
running on the same machine.
The port numbers selected must be from the reserved port
number range and have not been registered by another
application on this machine.

Please enter the port numbers.

Port Number for CVD : [8600]

Port Number for EvMgrC: [8602]
```

18. If this computer and the CommServe is separated by a firewall, type **Yes** and then press **Enter** to continue.

For firewall options and configuration instructions, see Firewall Configuration and continue with the installation.

If you do not wish to configure the firewall services, type **No** and then press **Enter** to continue.

```
Is there a firewall between this client and the CommServe?
[no]
```

19. Type the name of the CommServe computer and press **Enter** to continue.

NOTES

- Ensure that the CommServe is accessible before typing the name; otherwise the installation will fail.
- If you enter a short name which resolves to the same IP address as the fully qualified CommServe name, you will be asked if you would prefer to use the fully qualified name.

```
Please specify hostname of the CommServe below. Make sure
the hostname is fully qualified, resolvable by the name
services configured on this machine.

CommServe Host Name:
```

20. Enter the **username** and **password** information for an external domain user account or a CommCell user account. This authorizes the installation of an agent on the CommCell.

NOTES

- This is only displayed when the **Authentication for Agent** feature is enabled in the CommCell Properties. Users must belong to a User Group with Agent Management capabilities to enable this feature. For more information, see Authentication for Agent Installs.

Click **Enter** to continue.

```
Enter your CommCell user name and password:

User Name :

Password :

Press <ENTER> to continue ...
```

CONFIGURE INDEX CACHE

21. Specify the location for the MediaAgent's Index Cache.

NOTES

- You can accept the default or choose another location. In either case, the location must be local.
- If desired, you can change the index cache location to a network drive from the CommCell Console, any time after you have installed the MediaAgent software.
- The recommended minimum space required for the index cache directory is 256 MB.
- It is recommended that the index cache location to be on a partitioned drive used exclusively for holding an index cache.
- For information on calculating the space requirements for index cache, see Calculating the Storage Space Required for Index Cache.
- Do not specify the root directory as the index cache directory.

Press **Enter** to accept the default path and continue, or
Enter a path and then press **Enter** to continue.

```
MediaAgent maintains a cache of indices for completed
backups. Normally they're stored
in /test1/calypso/MediaAgent/IndexCache directory, but you
can keep them anywhere. You can even make an IndexCache
directory shared by two or more MediaAgents.

Please specify where you want us to store the Index Cache.

Cache Directory:
```

22. Press **Enter** to continue.

NOTES

```
Directory "/test1/calypso/MediaAgent/IndexCache" does not
exist.

Are you sure you entered its name correctly? [yes]
```

- This prompt is displayed when the specified Index Cache directory is not found.
  If you wish to specify another directory for Index Cache, type **No** and then press **Enter**.
  Specify the location for the MediaAgent's Index Cache.
- The index cache directory depends on the directory that you specified in the previous step and may appear different from the example shown.

SETUP COMPLETE

23. Press **Enter** to acknowledge the successful completion of the MediaAgent software installation.

```
Successfully installed CVGxMA.

Press ENTER to continue ...
```

24. If this is the last package that you wish to install/upgrade, enter the number corresponding to the **Exit** option and then press **Enter** to continue.

NOTES

- Only modules that are not installed/upgraded appear in the list.
- Your screen may appear different from the example shown.
- If you are installing on AIX, FreeBSD, IRIX or Tru64 computers, if this module was the last possible module to install, you are automatically exited from the program. Otherwise, type the number for the **Exit** option and then press **Enter.** The installation is completed.

```
Select the Calypso module that you would like to install.

1) FileSystem iDataAgent
2) Exit

Module number: [1]
```

25. This prompt is displayed only when you are installing on HP-UX or Linux, computers. Enter the number corresponding to the **Exit** option and then press **Enter** to continue.

The installation is now complete.

```
Certain Calypso packages can be associated with a virtual
IP, or in other words, installed on a "virtual machine"
belonging to some cluster. At any given time the virtual
machine's services and IP address are active on only one
of the cluster's servers. The virtual machine can "fail-
over" from one server to another, which includes stopping
services and deactivating IP address on the first server
and activating the IP address/services on the other
server.

Currently you have Calypso installed on physical node
stone.company.com.

Now you have a choice of either adding another package to
the existing installation or configure Calypso on a
virtual machine for use in a cluster.

1) Add another package to stone.company.com
2) Install Calypso on a virtual machine
3) Exit

Your choice: [1]
```

POST-INSTALL CONSIDERATIONS

GENERAL

- Review Install Considerations after installing the software.
- After installing the MediaAgent, if you wish to configure Kernel Parameters, see Kernel Parameter Configuration for more information.
- Install post-release updates or Service Packs that may have been released after the release of the software. When you are installing a Service Pack, ensure that it is the same version as the one installed in the CommServe Server. Alternatively, you can enable Automatic Updates for quick and easy installation of updates in the CommCell component.

Install the MediaAgent - Unix - Clustered Environment

TABLE OF CONTENTS

INSTALL REQUIREMENTS

The following procedure provides step-by-step instructions for installing the MediaAgent on a Unix cluster.

The software in a Unix cluster can be installed from the active node in the cluster group using the following procedure. Note that for a passive node in a Unix cluster, you need to install the software separately on the passive node in the cluster group.

For an overview of deploying the software components in a clustered environment, see Clustering Support.

Review the following Install Requirements before installing software on a Unix cluster:

GENERAL

- Review Install Considerations before installing the software.
- Agents should be installed only after the CommServe and at least one MediaAgent have been installed in the CommCell. Also, keep in mind that the CommServe and MediaAgent must be installed and running (but not necessarily on the same computer), before you can install the Agent.
- Ensure there is an available license on the CommServe for the Agent.
- Verify that you have the Software Installation Disc that is appropriate to the destination computer's operating system.

CLUSTER

- Refer to Installing the Software on the Cluster for important overview information about installing MediaAgent or Agent software in a Unix clustered environment.
- Check the following on the cluster computer in which you wish to install the software:
  - Cluster software is installed and running.
  - Active and passive nodes are available.
- Complete the following steps:
  1. Install the Base software and the required agents on all the nodes that are included in the cluster service. See Installation for more information.
  2. Be sure to install your software to the appropriate directories per the directives in UNIX Clusters.
  3. Verify that all of the computers to which software will be installed satisfy the minimum requirements specified in the appropriate System Requirements.
  4. Ensure that services are up and running on the remote hosts.

PACKAGE MANAGEMENT SYSTEMS

You can use the Red Hat Package Manager (RPM) package management system to install all Linux versions of the agent. Also, you can use the Advanced Packaging Tool (APT) package management system to install all Debian Linux versions of the agent. For step-by-step instructions, see Base Software Install for RPM Package Manager and Base Software Install for APT Package Manager.

HP-UX

If you are installing on a HP-UX computer, you must manually mount the installation disc as described in Mount the Software Installation Disc.

RED HAT LINUX

Red Hat Linux will create an entry in the `/etc/hosts` file when it is first installed, in the following format:

<ip_address> <host name> `localhost`

For example, if the host name of your computer is `bluesky`, the entry will look something like this:

```
192.168.1.111 bluesky localhost
```

If you have not already done so, edit the `/etc/hosts` file. The edited entry should look like this:

```
127.0.0.1 localhost
```

Depending upon your environment, and using the above example again, you may also need an entry similar to this:

```
192.168.1.111 bluesky
```

BEFORE YOU BEGIN

- Log on to the client as `root`.
- The install package requires `super-user` permissions to execute.

INSTALL PROCEDURE

GETTING STARTED

1. Place the software installation disc for the Unix platform into the disc drive.

   You can also install the product using a disc drive mounted on another computer on the network.

   - On Solaris, double-click the **cvpkgadd** program from the File Manager window.
   - On other Unix platforms, open the Terminal window, navigate to the software installation disc and then enter **./cvpkgadd**.

2. The product banner and other information is displayed.

   Press **Enter** to continue.

3. Read the license agreement. Type **y** and press **Enter** to continue.

4. Enter the number corresponding to the setup task you want to perform.

   NOTES

   - For Install data protection agents on this computer option, follow the steps described in this procedure.
   - Advance options provide additional setup features such as record and play setup, creating a custom package and External Data Connector Agent software.

     To create a custom package and for record and play setup, follow the steps described in Custom Package - Unix.

     To install the External Data Connector Agent, follow the steps described in External Data Connector - Unix.

```
Please select a setup task you want to perform from the
list below:

Advance options provide extra setup features such as
creating custom package, recording/replaying user
selections and installing External Data Connector
software.

1) Install data protection agents on this computer

2) Advance options

3) Exit this menu

Your choice: [1]
```

5. If your computer is 32-bit, press **Enter**.

   If your computer is 64-bit, see Install Unix Agents on 64-bit Platform for step-by-step procedure.

```
This machine supports both 32 bit and 64 bit binaries. By
default, we will install 32 bit binary set that has full
support for all the modules included in this package.
Please note that 64 bit binary set currently only support
limited modules.

1) All platforms (32 bit)

2) FS and MA only (64 bit)

Your choice: [1]
```

CLUSTER SELECTION

6. Type **2** and press **Enter** to install on a virtual machine.

```
Certain Calypso packages can be associated with a virtual
IP, or in other words, installed on a "virtual machine"
belonging to some cluster. At any given time the virtual
machine's services and IP address are active on only one
of the cluster's servers. The virtual machine can "fail-
over" from one server to another, which includes stopping
services and deactivating IP address on the first server
and activating the IP address/services on the other
server.

You now have a choice of performing a regular Calypso
install on the physical host or installing Calypso on a
virtual machine for operation within a cluster.

Most users should select "Install on a physical machine"
here.

1) Install on a physical machine

2) Install on a virtual machine

3) Exit

Your choice: [1]
```

7. Type the name of the virtual machine that you want to configure or its corresponding IP address and press **Enter**.

```
Please enter the hostname or IP address of the virtual
machine being installed. It can be either short or long;
the only requirement is that it must be resolvable by the
name services configured on this machine

WARNING: You should follow this path ONLY if this host
participates in a cluster and you really want to install
Calypso on the virtual machine. This is NOT how most
people will use Calypso.

If you got into this screen by mistake, hit ^C and restart
cvpkgadd.

Virtual Machine Host Name:
```

8. This prompt appears if you entered the short form of the virtual machine host name in the previous step. If you want to use the long form of the host name, accept the **yes** default; if not, type **no**. Then press **Enter**.

```
It looks like name "example.company.com" resolves to the
same IP as "example". Generally, it's better to use longer
name to address a host: less chances for name-to-IP
resolution problems on CommServe or other IDA/MA.

Would you like to use fully qualified
"example.company.com" instead of "example"?

Use longer "example.company.com" name? [yes]
```

9. If you have already installed the software on the virtual machine for the active node, accept the **yes** default to install for the passive node, press **Enter**, and go to the next step.

If you still must install for the active node, type **no**, press **Enter**, and perform the install for the virtual machine for the active node.

NOTES

- This prompt appears only when installing on a passive node.

```
When installing new Calypso packages on a virtual machine,
you should start with the active node, that is the host
where the virtual machine is currently running.

This node appears to be passive, so we will assume that
you have already installed Calypso for example.company.com
on the active node.

Is this correct? [yes]
```

10. Type the name of the virtual client and press **Enter**.

```
Please specify the client name for this machine.It does
not have to be the network host name: you can enter any
word here without spaces. The only requirement is that it
must be unique on the CommServe.

Virtual Machine Client Name: [hpuxmc1]
```

11. Specify the network interface that you want to associate with the physical machine and press **Enter**.

NOTES

- This prompt appears only when the Unix File System *i*DataAgent is not installed on the physical node.

```
Even though it is a virtual machine that you are
installing now, we still have to ask you to provide
hostname and client name for the physical node.

Network interfaces with the following IPs are available on
your system. Please select the one that you want to be
associated with Calypso physical machine. The interface
should be static, and should not get disabled in case of
cluster failover.

1) mackrel71
2) mackrel
3) mackrel1

Interface number: [1] 2
```

12. Verify the name of the physical interface and make any required changes. Then press **Enter**.

```
Please verify the physical interface name below. Make it
as complete (with fully qualified domain name) as
possible.

Physical Hostname: [mackrel]
```

13. Enter a node name for the physical machine and press **Enter**.

```
Even though you are installing Calypso on a machine, we
still need to ask you to provide a node name for the
physical machine.

It does not have to be the network host name: you can
enter any word here without spaces. The only requirement
is that it must be unique on the CommServe.

Physical Machine Node Name: [mackrel]
```

SELECT COMPONENTS FOR INSTALLATION

14. Enter the number corresponding to the **CVGxMA** module.

A confirmation screen will mark your choice with an "X". Type "d" for **Done**, and press **Enter** to continue.

NOTES

- To select multiple component, enter the number by adding a space.
- Your screen may look different from the example shown.
- Components that either have already been installed, or which cannot be installed, will not be shown.
- In addition, the list of modules that appear depends on the specific Unix File System in which the package is installed. (e.g., **CVGxWA** will appear only when the installation package is run on a Solaris computer.)

```
Install Calypso on physical machine client.company.com

Select the Calypso module that you would like to install

[ ] 1) Media Agent        [1301] [CVGxMA]
[ ] 2) FileSystem IDA     [1101] [CVGxIDA]
    >) >>>>> NEXT PAGE  >>>>>>

[a=all n=none r=reverse q=quit d=done >=next <=previous ?
=help]

Enter number(s)/one of "a,n,r,q,d,>,<,?" here: 2
```

BASE SOFTWARE INSTALLATION

15. If you wish to install the agent software for restore only, enter **Yes** and press **Enter** to continue. See Installing Restore Only Agents for more information.

    Otherwise, accept **no**, press **Enter** to continue.

```
Do you want to use the agents for restore only without
consuming licenses? [no]
```

16. Type the appropriate number to install the latest software scripts and press **Enter** to continue.

    NOTES

    - Select **Download from the software provider website** to download the latest software scripts from your software provider website.

      Make sure you have internet connectivity when you are using this option.
    - Select **Use the one in the installation media**, to install the software scripts from the disc or share from which the installation is performed.
    - Select **Use the copy I already have by entering its unix path**, to specify the path if you have the software script in an alternate location.

```
Installation Scripts Pack provides extra functions and
latest support and fix performed during setup time. Please
specify how you want to get this pack.

If you choose to download it from the website now, please
make sure you have internet connectivity at this time.
This process may take some time depending on the internet
connectivity.

1) Download from the software provider website.

2) Use the one in the installation media

3) Use the copy I already have by entering its unix path

Your choice: [1] 2
```

17. Enter **Yes** to download and install the latest service packs and post packs from the software provider.

    NOTES

    - Internet connectivity is required to download updates.
    - This step is applicable for multi instancing.

    Press **Enter** to continue.

```
Keep Your Install Up to Date - Latest Service Pack

Latest Service Pack provides extra functions and latest
support and fix for the packages you are going to install.
You can download the latest service pack from software
provider website.

If you decide to download it from the website now, please
make sure you have internet connectivity at this time.
This process may take some time depending on the internet
connectivity.

Do you want to download the latest service pack now? [no]

Press <ENTER> to continue ...
```

18. Specify the location where you want to install the software.

    NOTES

    - The amount of free space required depends on the components selected for install, and may look different from the example shown.

    Press **Enter** to accept the default path and continue, or
    Enter a path and then press **Enter** to continue.

    Press **Enter** again to confirm the path.

```
Please specify where you want us to install Calypso
binaries.

It must be a local directory and there should be at least
170MB of free space available. All files will be installed
in a "calypso" subdirectory, so if you enter "/opt", the
files will actually be placed into "/opt/calypso".

Installation Directory: [/opt]

..

Calypso will be installed in /opt/calypso.
Press ENTER to continue ...
```

19. Specify the location for the log files.

    NOTES

    - All the modules installed on the computer will store the log files in this directory.
    - The amount of free space required depends on the components selected for install, and may look different from the example shown.

    Press **Enter** to accept the default path and continue, or
    Enter a path and then press **Enter** to continue.

    Press **Enter** again to confirm the path.

```
Please specify where you want to keep Calypso log files.

It must be a local directory and there should be at least
100MB of free space available. All log files will be
created in a "calypso/Log_Files" subdirectory, so if you
enter "/var/log", the logs will actually be placed into
"/var/log/calypso/Log_Files".

Log Directory: [/var/log]

..

Calypso log files will be created
in /var/log/calypso/Log_Files.
Press ENTER to continue ...
```

20. Indicate whether you would like to launch processes with inherent database access rights.

    Press **Enter** to assign a new group, or
    Type **No** and then press **Enter** to continue.

```
Most of Calypso processes run with root privileges, but
some are launched by databases and inherit database access
rights. To make sure that registry and log files can be
written to by both kinds of processes we can either make
such files world-writeable or we can grant write access
only to processes belonging to a particular group, e.g. a
"calypso" or a "dba" group.

We highly recommend now that you create a new user group
and enter its name in the next setup screen. If you choose
not to assign a dedicated group to Calypso processes, all
temporary and configuration files will be created with -
rw-rw-rw permissions.

If you're planning to backup Oracle DB you should use
"dba" group.

Would you like to assign a specific group to Calypso?
[yes]
```

21. If you indicated **Yes** in the previous step, you will be prompted for the group name that must be used to launch processes.

    Enter the group name and then press **Enter** to continue.

    Press **Enter** again to continue.

    For installs on a Solaris computer, proceed to the next step. Otherwise, skip to Setup Complete.

```
Please enter the name of the group which will be assigned
to all Calypso files and on behalf of which all Calypso
processes will run.

In most of the cases it's a good idea to create a
dedicated "calypso" group. However, if you're planning to
use Oracle iDataAgent or SAP Agent, you should enter
Oracle's "dba" group here.

Group name: dba

REMINDER

If you are planning to install Calypso Informix, DB2,
PostgreSQL, Sybase or Lotus Notes iDataAgent, please make
sure to include Informix, DB2, etc. users into group
"dba".
Press <ENTER> to continue ...
```

22. Type a network TCP port number for the Communications Service (CVD) and press **Enter**.

Type a network TCP port number for the Client Event Manager Service (EvMgrC) and press **Enter**.

NOTES

- For more information about Network TCP Ports, see Network TCP Port Requirements.
- For more information about these services, see Services.
- If the port number you entered already exists, a message will be displayed `Port #### is already reserved in /etc/services`. To work around this issue, enter different port number.

```
Every instance of Calypso should use a unique set of
network ports to avoid interfering with other instances
running on the same machine.
The port numbers selected must be from the reserved port
number range and have not been registered by another
application on this machine.

Please enter the port numbers.

Port Number for CVD : [8600]

Port Number for EvMgrC: [8602]
```

23. If this computer and the CommServe is separated by a firewall, type **Yes** and then press **Enter** to continue.

For firewall options and configuration instructions, see Firewall Configuration and continue with the installation.

If you do not wish to configure the firewall services, type **No** and then press **Enter** to continue.

```
Is there a firewall between this client and the CommServe?
[no]
```

24. Type the name of the CommServe computer and press **Enter** to continue.

NOTES

- Ensure that the CommServe is accessible before typing the name; otherwise the installation will fail.
- If you enter a short name which resolves to the same IP address as the fully qualified CommServe name, you will be asked if you would prefer to use the fully qualified name.

```
Please specify hostname of the CommServe below. Make sure
the hostname is fully qualified, resolvable by the name
services configured on this machine.

CommServe Host Name:
```

25. Enter the **username** and **password** information for an external domain user account or a CommCell user account. This authorizes the installation of an agent on the CommCell.

NOTES

- This is only displayed when the **Authentication for Agent** feature is enabled in the CommCell Properties. Users must belong to a User Group with Agent Management capabilities to enable this feature. For more information, see Authentication for Agent Installs.

Click **Enter** to continue.

```
Enter your CommCell user name and password:

User Name :

Password :

Press <ENTER> to continue ...
```

KERNEL PARAMETERS

26. Enter the appropriate number of streams, and then press **Enter** to continue, or Press **Enter** to accept the default number of streams and continue.

NOTES

- The number of streams specified ensures that concurrent backup/restore streams would have sufficient system resources. For more information on the subject, see Configuring Kernel Parameters for Macintosh and Configuring Kernel Parameters for Solaris.

This prompt is relevant only when you install/upgrade on a Macintosh or Solaris computer as appropriate.

```
Please enter the total number of streams that you plan to
run at the same time. We need to make sure that you have
enough semaphores and shared memory segments configured
in /etc/system.

Number of streams: [10]
```

27. Indicate whether you would like modifications to be made to the `/etc/system` configuration file.

Type **Yes**, and then press **Enter** to automatically update the file and continue, or Press **Enter** to accept the default **No** and continue (if you do not want to automatically update the file).

This prompt is displayed only when you install/upgrade on a Solaris (8 or 9) or Macintosh computer.

```
We now need to modify the /etc/system configuration file
on this computer. It is done to make sure that there will
be enough shared memory and semaphores available for
Calypso programs.

Please review the changes below and answer "yes" if you
want us to apply them to the /etc/system file. Otherwise,
the installation will proceed, the changes will be saved
to some other file, and you will have to apply them
manually.

set shmsys:shminfo_shmmni=8570 (was 7930)
set shmsys:shminfo_shmseg=8420 (was 7780)
set semsys:seminfo_semmns=10320 (was 9680)
set semsys:seminfo_semmni=8570 (was 7930)
set semsys:seminfo_semmsl=8570(was 7930)

Do you want us to apply these changes now? [no]

Changes saved into /etc/system.gal.1744

Press <ENTER> to continue.
```

28. If you indicated **No** in the previous step, the file to which the changes have been

```
Although a 'no' answer can be selected to this question
```

saved is displayed.
Make sure that these values are established later to ensure that all the requirements for this setup is satisfied.

NOTES

- The settings that are displayed are the maximum or minimum required settings. Value ’640’, which is provided for various shared memory segment or semaphore requirements, is a maximum value based on 10 streams.

Press **Enter** to continue.

This prompt is displayed only when you install/upgrade on a Solaris (8 or 9) computer, in cases where the install detects that the computer does not have the maximum or minimum required shared memory settings.

```
during install, the user should make sure the min
requirements (below) for shared memory are met, otherwise
the backups may fail (the message in logs is ’could not
start the pipeline’).

set shmsys:shminfo_shmmax=4199304
set shmsys:shminfo_shmmin=1
set semsys:shminfo_shmmni=640
set semsys:shminfo_shmseg=640
set semsys:seminfo_semmns=640
set semsys:seminfo_semmni=640
set semsys:seminfo_semmsl=640
set maxusers=256
```

CONFIGURE MEDIAAGENT SPECIFIC INFORMATION

29. For a MediaAgent install on the active node only, accept or type the directory where you want to store the index cache and press **Enter**.

NOTES

- This prompt will not display for a MediaAgent install on a passive node.
- The index cache location that you enter should be shared by both the active node and the passive node.

```
MediaAgent maintains a cache of indices for completed
backups. Normally they're stored
in /opt/calypso/MediaAgent/IndexCache directory, but you
can keep them anywhere. You can even make an IndexCache
directory shared by two or more MediaAgents.

Please specify where you want us to store the Index Cache.

Index Cache Directory:
[/test1/calypso/MediaAgent/IndexCache] /satyr/Hp-Ux/Index
```

30. Press **Enter** to continue.

```
.....
.....
.....

Successfully installed CVGxMA.

Press ENTER to continue ...
```

SETUP COMPLETE

31. If this is the last package that you wish to install/upgrade, enter the number corresponding to the **Exit** option and then press **Enter** to continue.

NOTES

- Only modules that are not installed/upgraded appear in the list.
- Your screen may appear different from the example shown.
- If you are installing on AIX, FreeBSD, IRIX or Tru64 computers, if this module was the last possible module to install, you are automatically exited from the program. Otherwise, type the number for the **Exit** option and then press **Enter.** The installation is completed.

```
Select the Calypso module that you would like to install.

1) FileSystem iDataAgent
2) Exit

Module number: [1]
```

32. This prompt is displayed only when you are installing on HP-UX, Linux, or Solaris computers. Enter the number corresponding to the **Exit** option and then press **Enter** to continue.

The installation is now complete.

```
Calypso is currently configured on virtual machine
hpuxmc1.company.com.

Now you have an option of installing Calypso on physical
machine, another virtual machine or you can add a new
package to hpuxmc1.company.com.

1) Add a new package to hpuxmc1.company.com
2) Install Calypso on the physical machine
3) Install Calypso on another virtual machine
4) Exit

Your choice: [1]
```

POST-INSTALL CONSIDERATIONS

GENERAL

- Install post-release updates or Service Packs that may have been released after the release of the software. When you are installing a Service Pack, ensure that it is the same version as the one installed in the CommServe Server. Alternatively, you can enable Automatic Updates for quick and easy installation of updates in the CommCell component.
- After installing the MediaAgent, if you wish to configure Kernel Parameters, see Kernel Parameter Configuration for more information.

CLUSTER

- The cvclusternotify script should be added as part of the normal cluster startup/shutdown procedure. The script is provided as a generic template, and it must be run at the beginning of node shutdown and at the end of new active node startup. In both cases, data protection services must be up and running.

  Run the following command to notify Calypso that the specified "virtual node" is going up or down because of a cluster failover:

  Usage:

```
cvclusternotify -inst <Instance> -cn <Client Name> -start|-shutdown
```

Where:

`cvclusternotify` - Program to notify Calypso of cluster failovers

Example:

For two-node cluster, if the virtual client name is "virtual" and the application instance is "Instance001", run the following command:

- To shutdown:

  ```
  cvclusternotify -inst Instance001 -cn "virtual" -shutdown
  ```

- To start up:

  ```
  cvclusternotify -inst Instance001 -cn "virtual" -start
  ```

- On failover of a Linux cluster, Services may be killed by cluster services during a virtual machine failover. To insure that the Services are re-started on the passive node, add commands in failover scripts to start Services.

DISASTER RECOVERY CONSIDERATIONS

- Before you use your agent, be sure to review and understand the associated full system restore (or disaster recovery) procedure. The procedure for some agents may require that you plan specific actions or consider certain items before an emergency occurs. See Disaster Recovery for more information regarding your agent.

Library and Drive Configuration

Topics | How To | Troubleshoot | Related Topics

OVERVIEW

You can open the **Library and Drive Configuration** window from the CommCell Console. You can access this window from CommCell Console of the Control Panel.

The **Library and Drive Configuration** window is used to perform the following operations on all supported libraries in the selected MediaAgents.

- **Display**

  To display the existing libraries and drives that are configured for the selected MediaAgent(s).

- **Detect Devices**

  Use the Detect Devices option to display the detect status for all devices that are controlled by MediaAgents.

- **Configure libraries, master drive pools, drive pools, and drives**

  Library configuration enables MediaAgents to utilize the library as storage resources. Master drive pool and drive pool configuration creates the necessary entries for these entities in the CommServe database. Drive configuration enables a MediaAgent to read and write data through the media drive.

- **Share libraries among MediaAgents**

  In order to share a library among MediaAgents, either directly or via a Storage Area Network (SAN), you must properly configure and map the resident drives. The **Library and Drive Configuration** window can be used for this purpose and also if you want to modify the configuration of a shared library.

- **Discover media**

  In order to use the media within a library, the MediaAgent must collect information about the new media and update the media database through the discovery process.

- **Validate the SCSI mapping of devices within the CommCell**

  The Validate feature verifies that the MediaAgent has access to each physical device through the device’s mapped SCSI address. During the validation process, the MediaAgent mounts a media into the selected drive(s) and displays a status message indicating whether the operation succeeded.

- **Change the SCSI mapping of storage devices**

  The **Library and Drive Configuration** window supports the manual process to deal with SCSI changes on the library and drives, if necessary. The SCSI hardware issues involved in library and drive configuration are explained in detail in each of the library configuration sections.

  The MediaAgent detects any SCSI changes when you stop and re-start the services as described in Update the SCSI address of a configured library within the CommServe database. You can also verify whether the SCSI configuration of devices within the CommCell correctly matches the current configuration, by performing an exhaustive detection operation as described in Detect Devices Using Exhaustive Detection.

  If there are any major changes to the hardware that affects your existing SCSI mapping, such as replacing a library, follow the appropriate procedure described in Hardware Changes.

- **View properties of libraries, master drive pools, drive pools, and drives**

Configuration information of libraries, master drive pools, drive pools and drives can be viewed from the **Library and Drive Configuration** window.

- **Deconfigure libraries, master drive pools, drive pools, and drives**

  Deconfiguring a library or drive disables software communications between the MediaAgent and the device. For comprehensive information, see Deconfiguring Libraries and Drives.

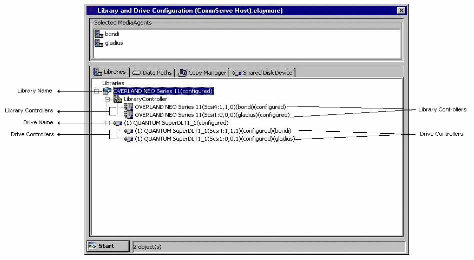
UNDERSTANDING THE LIBRARY AND DRIVE CONFIGURATION WINDOW

The **Library and Drive Configuration** window displays several tabs. Each of these tabs can are used for distinct purposes as described in the following sections.

LIBRARIES

The **Libraries** tab displays the configured devices such as the libraries, library controllers, drives and drives controllers. This view provides a physical view of a library and its drive along with information on the library and drive controllers accessing them. This view facilitates faster browsing of devices especially in a SAN environment and for libraries with dual HBA cards.

The image on the right highlights some of the important information displayed in the **Libraries** tab.



Library and Drive Configuration (CommServe Host):claymore)

Selected MediaAgents

bondi
gladius

Libraries | Data Paths | Copy Manager | Shared Disk Device

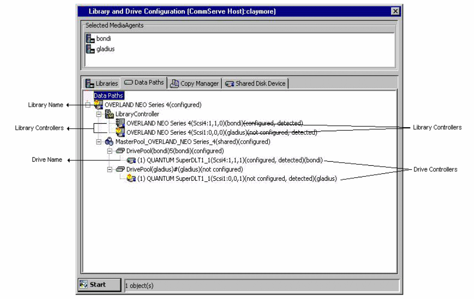
```
Libraries
OVERLAND NEO Series 11(configured)
  LibraryController
    OVERLAND NEO Series 11(Scsi4:1,1,0)(bondi)(configured)
    OVERLAND NEO Series 11(Scsi1:0,0,0)(gladius)(configured)
  (1) QUANTUM SuperDLT1_1(configured)
    (1) QUANTUM SuperDLT1_1(Scsi4:1,1,1)(configured)(bondi)
    (1) QUANTUM SuperDLT1_1(Scsi1:0,0,1)(configured)(gladius)
```

Start | 2 object(s)

DATA PATHS

The **Data Paths** tab displays a detailed view of a library and its drives which includes all the master drive pools and drive pools that are configured to access them. Once configured the window displays all the logical data paths to the devices.

The image on the right highlights some of the important information displayed in the **Data Paths** tab.



Library and Drive Configuration (CommServe Host):claymore)

Selected MediaAgents

bondi
gladius

Libraries | Data Paths | Copy Manager | Shared Disk Device

```
Data Paths
OVERLAND NEO Series 4(configured)
  LibraryController
    OVERLAND NEO Series 4(Scsi4:1,1,0)(bondi)(configured, detected)
    OVERLAND NEO Series 4(Scsi1:0,0,0)(gladius)(not configured, detected)
  MasterPool_OVERLAND_NEO Series_4(shared)(configured)
    DrivePool(bondi)5(bondi)(configured)
      (1) QUANTUM SuperDLT1_1(Scsi4:1,1,1)(configured, detected)(bondi)
    DrivePool(gladius)#(gladius)(not configured)
      (1) QUANTUM SuperDLT1_1(Scsi1:0,0,1)(not configured, detected)(gladius)
```

Start | 1 object(s)

COPY MANAGER

The **Copy Manager** tab allows you to detect and configure all eligible copy manager devices. Once configured the Copy Manager Devices are displayed in the window.

The image on the right highlights some of the important information displayed in the **Copy Manager** tab.

SHARED DISK DEVICE

The **Shared Disk Device** tab allows you to detect and configure the shared disk devices in the CommCell. Once configured the configured devices are displayed in the Window.

The image on the right highlights some of the important information displayed in the **Shared Disk Device** tab.

The following table lists the levels in the **Data Paths** tab tree, together with the information that is presented at each level.

LEVEL IN TREE	INFORMATION DISPLAYED	DETAILS
Library (tape or optical libraries only)	library name	The default library name includes the library manufacturer and model.
	media changer SCSI ID	Complete SCSI ID (including SCSI card number, bus, target, and LUN) of the library’s media changer.
	associated MediaAgent	The MediaAgent that controls the media changer in the library.
	configuration and detection status	See Detection and Configuration for detailed information.
Master Drive Pool (tape or optical libraries only)	master drive pool name	
	configuration status	See Detection and Configuration for detailed information.
Drive Pool (tape or optical libraries only)	drive pool name	
	associated MediaAgent	The MediaAgent that controls the drives belonging to this drive pool.
Drive (tape or optical libraries only)	physical location	The number by which the library identifies the drive internally.
	drive name	The default drive name includes the drive manufacturer and model.
	SCSI ID	Complete SCSI ID (including SCSI card number, bus, target, and LUN) of the drive.
	configuration and detection status	See Detection and Configuration for detailed information.
Library (disk)	library name	
	associated MediaAgent	The MediaAgent that control the disk library.
Mount Path (disk only)	mount path number	The number by which the MediaAgent identifies the mount path, internally.
	path	File system path for disk storage.

UNDERSTANDING SCSI MAPPINGS IN THE LIBRARY AND DRIVE CONFIGURATION WINDOW

In order to understand the information that follows, you should be able to differentiate between the following items of drive-related information:

- **Drive numbers**

  Libraries with multiple drives, number the drives, based on its physical location. (drive slots) This is used by the MediaAgent for internal identification. Different libraries follow different conventions; drives may be numbered from left to right or top to bottom, physically labeled on the outside of the library, etc. See the library's vendor documentation for the numbering conventions used.

- **SCSI address**

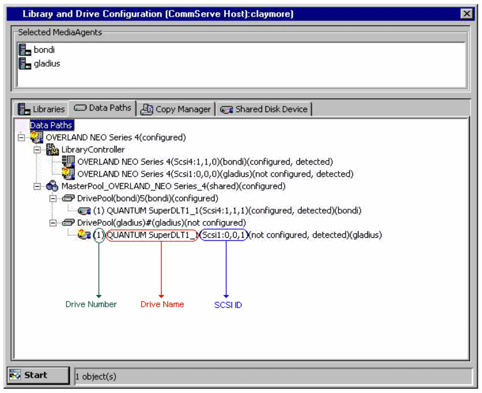
  This is the complete SCSI address (including bus, target, logical unit number (LUN) and PCI port number) through which the MediaAgent attempts to access a device.

- **Drive name**

  The MediaAgent initially assigns a drive name which is derived from the drive manufacturer and model.

  You can change the name of a drive by providing an alias at any point. We recommend that you give each drive a descriptive name, for easier system administration.

The sample image on the right shows each of these items as it appears in the **Library and Drive Configuration** window.



Library and Drive Configuration (CommServe Host):claymore)

Selected MediaAgents

bondi

gladius

Data Paths

OVERLAND NEO Series 4(configured)

LibraryController

OVERLAND NEO Series 4(Scsi4:1,1,0)(bondi)(configured, detected)

OVERLAND NEO Series 4(Scsi1:0,0,0)(gladius)(not configured, detected)

MasterPool_OVERLAND_NEO Series_4(shared)(configured)

DrivePool(bondi)5(bondi)(configured)

(1) QUANTUM SuperDLT1_1(Scsi4:1,1,1)(configured, detected)(bondi)

DrivePool(gladius)#(gladius)(not configured)

(1) QUANTUM SuperDLT1_1(Scsi1:0,0,1)(not configured, detected)(gladius)

1 object(s)

Although the library's display of the drive numbers may start with a number other than 1 (e.g., 0), the MediaAgent always starts numbering physical locations within a library from 1.

Ensure that the actual SCSI numbers and drive numbers in the library correspond to the SCSI numbers and drive numbers displayed for the library in the **Library and Drive Configuration** window. If you are not sure, or if there is a mismatch, run the exhaustive detection process. For information on performing exhaustive detection on libraries and drives, see Detect Devices Using Exhaustive Detection.

DEVICE DETECTION

Detection is the process by which the selected set of MediaAgents, on which the detection process is run, establishes hardware communications with storage devices. Device detection is of two types; Detection, and Exhaustive Detection.

DETECTION

When a device has `detect success` status, it indicates that the system has all of the information necessary to use the device. Note that the system only detects devices for which device drivers are loaded. A device may also have the following status:

- `partially configured, detect fail - connection error` status when the detection fails due to an error connecting to the MediaAgent
- `partially configured, detect fail - device not found` status if the detection fails due to a missing device
- `cannot find a matching device` status if the SCSI address for the device is changed

See Detect Devices for step-by-step instructions.

Note that some devices (e.g., the library associated with a stand-alone drive) have no detection status, since they are virtual entities and as such have no hardware components that can be detected.

On AIX MediaAgents, the presence of a number of SCSI adaptors may result in slowing down the detection process. If you know that some of these adaptors are not required by the MediaAgent you can skip them during the detection process. See Device Detection on AIX MediaAgent is Slow for more information.

EXHAUSTIVE DETECTION

Exhaustive detection is a process of associating drive numbers to its correct SCSI address. This is done by mounting a media to each of the drives in the library to obtain the drive's SCSI address. The following icons are displayed in the **Library and Drive Configuration** window, depending on whether devices were successfully identified:

This icon is displayed for libraries and drives that were successfully identified during the exhaustive detection process. This indicates that the devices were successfully detected but not configured. (all configured devices have no icons.)

This icon is displayed for drive slots that are either empty, not detected or cannot be detected on the selected MediaAgent

This icon indicates that the exhaustive detection option was not selected and hence the detection process has performed a SCSI detect of the devices and made a best guess by associating drives and libraries to arrive at a tree structure.

We strongly recommend that you perform an exhaustive detection of the devices the first time you configure the libraries and drives. When you start the exhaustive detection operation, the system will detect all the libraries (and drives) attached to selected MediaAgent(s). See Detect Devices Using Exhaustive Detection on all Devices Controlled by the MediaAgent(s) for step-by-step instructions.

This process attempts to mount a media in each of the selected drives to determine the drive numbers to its correct SCSI address. Due to the nature of this operation and depending on the number of drives, the time it takes to complete this operation may vary.

This procedure cannot be used for detecting stand-alone drives.

After the initial configuration, exhaustive detection can be performed at the Library/Drive/Library Controller levels, in the following situations:

- When you make changes to the existing devices. e.g., adding or removing drives or libraries.
- When you configure libraries with missing devices.

If the library and drive configuration has changed extensively and the library does not support the drive identifiers then perform the operation at the library level; for minor changes at the drive level, perform the operation at the drive level. See Detect Devices Using Exhaustive Detection on a Specific Library/Drive/Library Controller for step-by-step instructions.

DETECTION FOR LIBRARIES THAT SUPPORT SCSI 3 DRIVE IDENTIFICATION INFORMATION

If the library supports SCSI 3 the library can be configured without performing exhaustive detection.

To verify whether the library supports SCSI 3, run the `ScanScsiTool.exe` from the command prompt.

This tool is available in the following locations:

- Windows: `<`*`Software Installation Path`*`>\Base`
- Unix: `<`*`Software Installation Path`*`>/Base/ScanScsiTool`

If SCSI 3 is supported, the Drive Identifiers will be displayed under the Library Information. You will notice that when SCSI 3 is present, a regular detection (as opposed to an exhaustive detection) will display the yellow question mark icon in the **Library and Drive Configuration** window, when the devices were successfully identified.

CONFIGURATION

Configuration is the process by which the MediaAgent software collects the information that is needed for software support of a device. This process must be performed in the **Library and Drive Configuration** window.

When a device has a `configured` status, it indicates that the MediaAgent has all of the information necessary to use the device.

If you have to share the same physical library between multiple CommCells, the library needs to be virtualized so that one virtual partition is assigned to a given CommCell. This can be achieved using library vendor provided options.

CONFIGURING LIBRARIES AND DRIVES FROM THE COMMAND LINE USING SCANSCSITOOL

The Scanscsitool can be used to configure Shared Disk and tape libraries from command line. The following section describes the command line and the option available to this tool:

To configure tape libraries:

1. From the command prompt, navigate to *<Software_Installation_Directory>\Base* folder.
2. Run the following command:

   Usage:

   ```
   C:\Program Files\Company\Software\Base> ScanScsiTool.exe [option1|option2|...]
   ```

To create Shared Disk Library:

1. From the command prompt, navigate to *<Software_Installation_Directory>\Base* folder.
2. Run the following command:

   Usage:

   ```
   ScanSCSITool -h <MediaAgent Name> -a <Magnetic_Library_Name> -f <Mount Path>
   ```

   For Windows, you can also provide UNC Path when creating a shared disk library:

   ```
   ScanSCSITool -h <MediaAgent Name> -a <Magnetic_Library_Name> -useUNC -f <UNC Path> -u <UserName> -p <Password>
   ```

   Example:

   ```
   C:\Program Files\Company\Software\Base>scanscsitool -h giant -a "SCSIMagLib" -f "D:\0113\Maglib_mountpath"
   ```

   ```
   C:\Program Files\Company\Software\Base>scanscsitool -h giant -a "SCSIMagLib" -useUNC -f "\\scorpio\D\01132011\Magli_mountpath" -u scorpio\administrator -p password1
   ```

Scanscsi tool is used to create a shared disk library with one MediaAgent. To share the device with multiple MediaAgents, see Configure Multiple MediaAgents for a Static Shared Disk Device for step-by-step instruction.

Options:

Host Options:

`-h<hostname>`	MediaAgent Name
`-i<instanceName>`	Instance Name

Auto Config options for MediaAgent (with '-h' option):

`-n<libraryName>`	Library Alias Name, if set, only configure the matched library
`-l<libraryID>`	Library ID, if libraryID = 0, all detected libraries will be configured
`-s<libSerial#>`	Library serial number, if not set, all detected libraries will be configured
`-a<magLibraryName>`	Disk Library Alias Name, if set, only configure the matched disk library
`-m<magLibraryId>`	Disk Library ID, if not set, a new Disk Library will be configured
`-f<mountpath>`	Mount path
`-u<username>`	User name for network mount path
`-p<password>`	Password for network mount path
`-useUNC`	To use UNC Path as mount path (For Windows only)

Validating Drives in a Library

When the validation process is performed from the **Library and Drive Configuration** window, the system identifies the drives in the library. During the validation process, for each drive, the system randomly picks up a media from one of the slots in the library and uses it to validate the drives. Every drive may use the same or a different media, depending on the randomization. Drive validation can be performed from the library, master drive pool, drive pool or from the individual drive.

Drive validation is not supported for optical libraries and libraries with WORM media.

Another form of drive validation can be performed from the CommCell Console. See Validate Drive for more details.

Migrating Tape Library to a New MediaAgent

When tape library has been moved to the new MediaAgent, use the following steps to migrate the tape library to a new MediaAgent.

1. From the CommCell Console, click the **Tools** menu and then click **Control Panel**.
2. From the Control Panel, double-click the **Library & Drive Configuration**.
3. From the Select MediaAgents dialog box, select the following:
   - Select the MediaAgent(s) whose devices you want to detect or display from the **Available MediaAgents** list box.
   - Click **Add >>** to move the MediaAgent(s) to the Selected MediaAgents list box.
   - Click **OK**.
4. Click **OK**.
5. Once you attach the library to the new MediaAgent, use the steps described in Detect Devices to detect devices for new MediaAgent.
6. For existing MediaAgent the library will appear as configured.

   Use the steps described in Deconfigure Libraries to deconfigure the library. Once deconfigured the status of the library appear as not configured.

   Use the steps described in Delete Deconfigured Libraries to delete the library.
7. To use the new Tape library, change the data path on the Storage Policy Copy which was previously used by existing library.

   See Change Data Path on Storage Policy Copy for step-by-step instructions.

Discovering Media

Before using a new media, the system must collect certain information about it through a process known as discovery. When a media has been discovered its information is entered into the CommServe database. Media can be discovered from both the **Library and Drive Configuration** window and the **CommCell Browser**. For comprehensive information on discovering media, see Discover Media.

USE QPROFILE UTILITY TO DISPLAY DRIVE UTILIZATION OR LIBRARY JOB DETAILS

The QProfile utility in the Resource Pack can be used to show the drive utilization or attempts and failures of library jobs per a given interval. This utility will generate a report of the jobs associated with library jobs for a given time period. To obtain additional details regarding the given jobs, select the Details check box.

Back to Top

Library and Drive Configuration - How To

Topics | How To | Troubleshoot | Related Topics

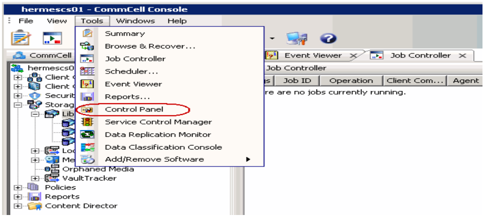
DISPLAY THE LIBRARY AND DRIVE CONFIGURATION WINDOW

The following procedure describes the steps involved in displaying the `Library and Drive Configuration` window.

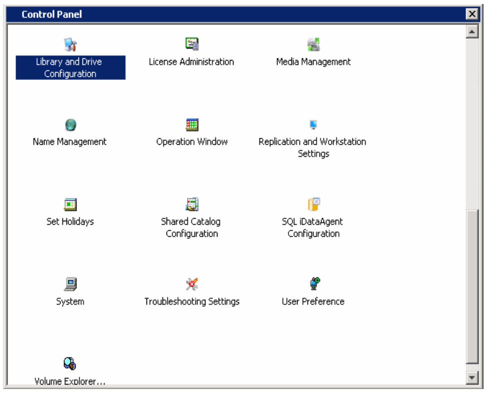
Required Capability: See Capabilities and Permitted Actions

TO DISPLAY THE LIBRARY AND DRIVE CONFIGURATION WINDOW

1. From the **Tools** menu in the CommCell Console, click **Control Panel**.

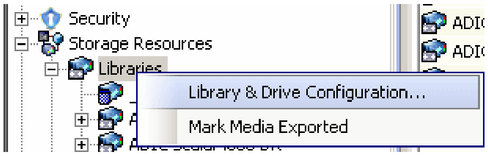


Double click **Library & Drive Configuration**.



2. Alternatively, from the **CommCell Browser**, right-click **Libraries** under **Storage**

Resources node, and then click **Library & Drive Configuration...**

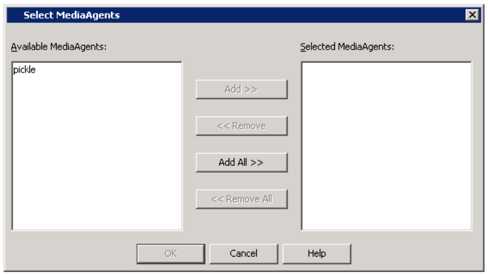


3. Select the MediaAgent(s) whose devices you want to detect or display, and then click **OK.**

   To configure any shared library, make sure you select all the MediaAgents that share the library.

   NOTES

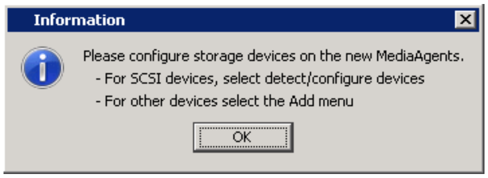
   - If a device has already been configured for the MediaAgent, the system displays the device in the **Library & Drive Configuration** window.
   - For cluster, select the cluster server as the MediaAgent.



4. Click **OK** to continue.

   NOTES

   - The system displays this prompt only if a library is not configured. Subsequently the **Library and Drive Configuration** window displays a blank screen.
   - If a library is already configured, this prompt is not displayed. Subsequently the detected devices are displayed with detection status **detect success** in the **Library and Drive Configuration** window.


Information

Please configure storage devices on the new MediaAgents.
- For SCSI devices, select detect/configure devices
- For other devices select the Add menu

You can now detect the devices controlled by the selected MediaAgent(s) as described in Detect Devices.

DETECT DEVICES

Related Topic

- Detection

The following procedure describes the steps involved in detecting the devices attached to a MediaAgent.

BEFORE YOU BEGIN

- Verify that the necessary SCSI adapters and drivers for the library attached to the MediaAgent computer are installed.
- Check and verify that the hardware is visible to the operating system. For a more detailed explanation on verifying the driver configurations, see the following sections:
  - Hardware Configuration Guidelines - Direct-Attached Library
  - Hardware Configuration Guidelines - Direct-Attached Shared Library
  - Hardware Configuration Guidelines - Libraries Attached to a SAN
- Ensure that the CommServe computer and library are accessible.

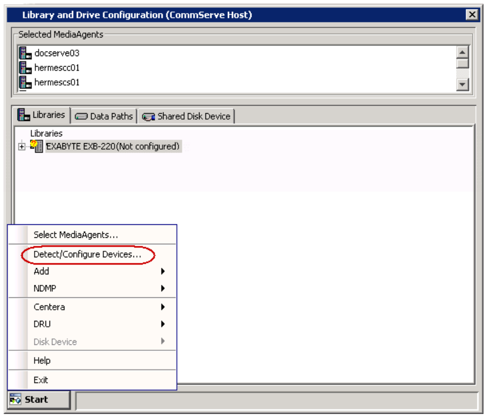
  CAUTION

  Before configuring the libraries and drives in SAN, we strongly recommend you to verify and ensure that proper hardware zoning of tape drives be implemented, especially when you have HBA fail over implemented in your environment. For more information on zoning of HBA fail over, contact your HBA software vendor.
- This feature requires a Feature License to be available in the CommServe® Server.

  Review general license requirements included in License Administration. Also, View All Licenses provides step-by-step instructions on how to view the license information.

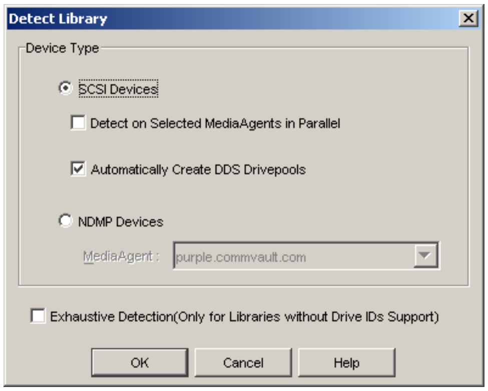
TO DETECT DEVICES CONTROLLED BY MEDIAAGENT(S)

1. Display the Library and Drive Configuration window.
2. From the **Library and Drive Configuration** window, click the **Start** menu and choose **Detect/Config Devices**.



3. In the **Detect Library** dialog box, choose the appropriate options:
   - **SCSI Devices** - If your library is attached to the SCSI or Fiber Channel (FC) Adapter.
   - **Detect on Selected MediaAgents in Parallel** - If you are performing the detection for multiple MediaAgents.
   - **Automatically create DDS Drivepools** - If your library is attached to multiple MediaAgents in a SAN environment.
   - **NDMP Devices** - If your library is attached to a NAS filer.
   - **Exhaustive Detection** - Only for libraries without Drive IDs support.

   Click **OK**.


Detect Library

Device Type

● SCSI Devices

□ Detect on Selected MediaAgents in Parallel

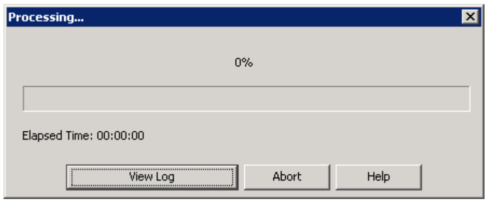
☑ Automatically Create DDS Drivepools

○ NDMP Devices

MediaAgent : purple.commvault.com

□ Exhaustive Detection(Only for Libraries without Drive IDs Support)

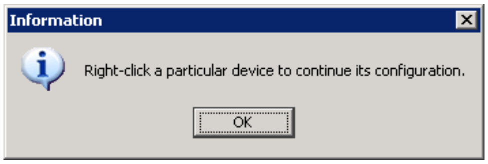
4. Optionally, from the **Processing** dialog box you can perform the following operations:
   - Click the **Abort** button to abort the exhaustive detection operation and unmount any mounted media from the drives.
   - Click the **View Log** button to display the **Log** dialog box which reports the status of each task that is performed during the exhaustive detection operation.


Processing...

0%

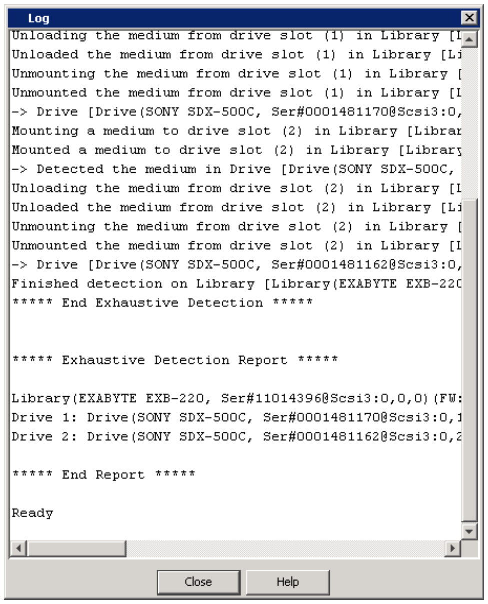
Elapsed Time: 00:00:00

5. An **Information** prompt appears, informing you to right-click the device to continue the configuration. Click **OK** to proceed.


Information

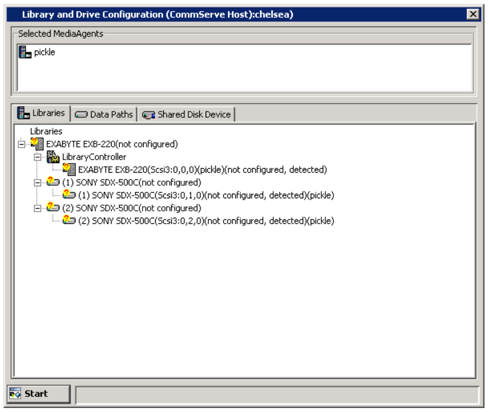
Right-click a particular device to continue its configuration.

6. When the detection process is completed, the log file is displayed. Note the log file contents and click **Close** to proceed.



```
Unloading the medium from drive slot (1) in Library [L
Unloaded the medium from drive slot (1) in Library [Li
Unmounting the medium from drive slot (1) in Library [
Unmounted the medium from drive slot (1) in Library [L
-> Drive [Drive(SONY SDX-500C, Ser#0001481170@Scsi3:0,
Mounting a medium to drive slot (2) in Library [Librar
Mounted a medium to drive slot (2) in Library [Library
-> Detected the medium in Drive [Drive(SONY SDX-500C,
Unloading the medium from drive slot (2) in Library [L
Unloaded the medium from drive slot (2) in Library [Li
Unmounting the medium from drive slot (2) in Library [
Unmounted the medium from drive slot (2) in Library [L
-> Drive [Drive(SONY SDX-500C, Ser#0001481162@Scsi3:0,
Finished detection on Library [Library(EXABYTE EXB-220
***** End Exhaustive Detection *****


***** Exhaustive Detection Report *****

Library(EXABYTE EXB-220, Ser#11014396@Scsi3:0,0,0)(FW:
Drive 1: Drive(SONY SDX-500C, Ser#0001481170@Scsi3:0,1
Drive 2: Drive(SONY SDX-500C, Ser#0001481162@Scsi3:0,2

***** End Report *****

Ready
```

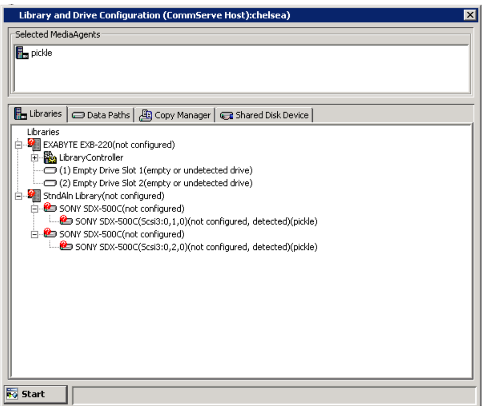
7. If the library supports SCSI 3 drive identification, the system detects the devices and displays them with detection status **detect success**, in the **Library and Drive Configuration** window. Configure the library as described in Configure Devices.



```
pickle

Libraries
  EXABYTE EXB-220(not configured)
    LibraryController
      EXABYTE EXB-220(Scsi3:0,0,0)(pickle)(not configured, detected)
    (1) SONY SDX-500C(not configured)
      (1) SONY SDX-500C(Scsi3:0,1,0)(not configured, detected)(pickle)
    (2) SONY SDX-500C(not configured)
      (2) SONY SDX-500C(Scsi3:0,2,0)(not configured, detected)(pickle)
```

If the library does not support SCSI 3 drive identification, the system detects the Library with **Empty Drive Slots** and the drives as **StndAln Library**.

Perform an Exhaustive Detection before configuring the library. (See Detect Devices Using Exhaustive Detection for step-by-step instructions.)



```
pickle

Libraries
  EXABYTE EXB-220(not configured)
    LibraryController
    (1) Empty Drive Slot 1(empty or undetected drive)
    (2) Empty Drive Slot 2(empty or undetected drive)
  StndAln Library(not configured)
    SONY SDX-500C(not configured)
      SONY SDX-500C(Scsi3:0,1,0)(not configured, detected)(pickle)
    SONY SDX-500C(not configured)
      SONY SDX-500C(Scsi3:0,2,0)(not configured, detected)(pickle)
```

DETECT DEVICES USING EXHAUSTIVE DETECTION ON ALL DEVICES CONTROLLED BY THE MEDIAAGENT(S)

Required Capability: See Capabilities and Permitted Actions

BEFORE YOU BEGIN

- Review Exhaustive Detection.
- Verify that the necessary SCSI adapters and drivers for the library attached to the MediaAgent computer are installed.

  If you have two libraries with different drive types (e.g. AIT and DLT 4000 drive types) and even if you do not plan to use some of the drives, ensure that all the drivers associated with all the drives types are installed. In some cases, if you do not install all the appropriate drivers, the device configuration may fail.

Consider the following:

- In a SAN environment you may have libraries with two different drive types connected to your bridge or switch (e.g., AIT and DLT 4000 drive types) If you planned on using only the DLT 4000 drives and hence only installed the drivers for the DLT 4000 drives, you would not be able to configure these drives in the **Library and Drive Configuration** window, until you install the drivers associated with all the other drive types (AIT) in the libraries.
- If you have an existing library (e.g. a library with DLT 4000 drives) which is already configured, and if you add another library with another drive type into your environment (e.g. a library with AIT drives) the SCSI ID of the configured library may change and you may need to edit the address in the properties of the devices in the **Library and Drive Configuration** window.

- Check and verify that the hardware is visible to the operating system. For a more detailed explanation on verifying the driver configurations, see the following sections:
  - Hardware Configuration Guidelines - Direct-Attached Libraries
  - Hardware Configuration Guidelines - Direct-Attached Shared Library
  - Hardware Configuration Guidelines - Libraries Attached to a SAN
- Ensure that the CommServe computer and library are accessible.
- As this operation may involve the mounting of a media in a drive, ensure that media is available in the library. Also ensure that the media is not a cleaning media.
- Exhaustive detection should not be performed when other jobs are using the drives in the library. Stop all jobs before performing an exhaustive detection.
- Verify and ensure that no media is mounted in the drives available in the libraries connected to the selected MediaAgent(s).

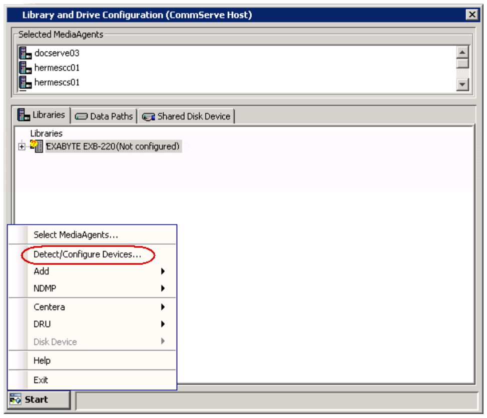
CAUTION

Before configuring the libraries and drives in SAN, we strongly recommend you to verify and ensure that proper hardware zoning of tape drives be implemented, especially when you have HBA fail over implemented in your environment. For more information on zoning of HBA fail over, contact your HBA software vendor.

TO DETECT DEVICES CONTROLLED BY MEDIAAGENT(S)

1. Display the Library and Drive Configuration window.

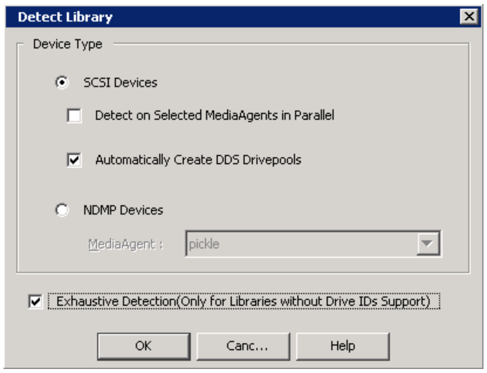
2. From the **Library and Drive Configuration** window, click the **Start** menu and choose **Detect/Config Devices**.



3. In the **Detect Library** dialog box, choose the appropriate options:

- **SCSI Devices** - If your library is attached to the SCSI or Fiber Channel (FC) Adapter.
- **Detect on Selected MediaAgents in Parallel** - If you are performing the detection for multiple MediaAgents.
- **Automatically create DDS Drivepools** - If your library is attached to multiple MediaAgents in a SAN environment.
- **NDMP Devices** - If your library is attached to a NAS filer.
- **Exhaustive Detection** - Only for libraries without Drive IDs support.

Click **OK**.


Detect Library

Device Type

● SCSI Devices

□ Detect on Selected MediaAgents in Parallel

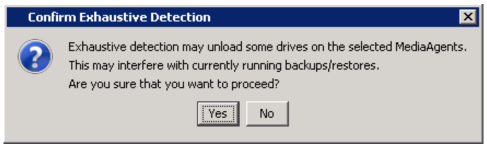
☑ Automatically Create DDS Drivepools

○ NDMP Devices

MediaAgent : pickle

☑ Exhaustive Detection(Only for Libraries without Drive IDs Support)

4. Click **Yes** to continue.

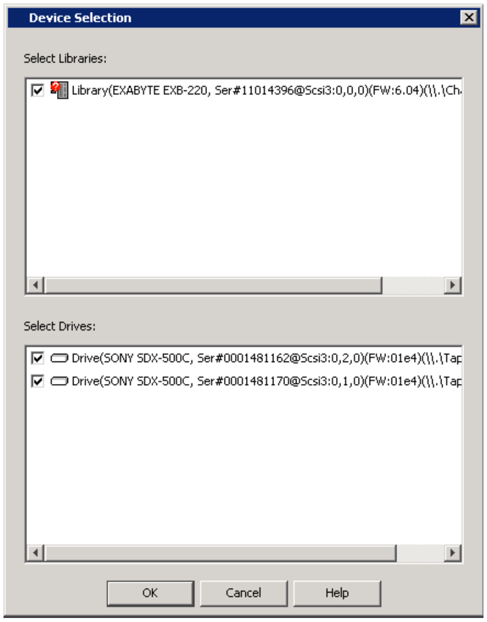

Confirm Exhaustive Detection

Exhaustive detection may unload some drives on the selected MediaAgents.
This may interfere with currently running backups/restores.
Are you sure that you want to proceed?

5. From the **Device Selection** dialog box, select the libraries and drives you wish to detect and then click **OK**.

The detection process will attempt to detect the devices by mounting the media in each of the selected drives to determine the correct drive to library mapping.

You can track the progress of the operation in the **Processing** dialog box.



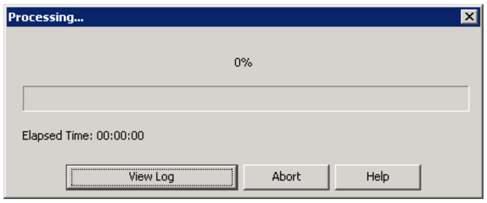
Select Libraries:

☑ Library(EXABYTE EXB-220, Ser#11014396@Scsi3:0,0,0)(FW:6.04)(\\.\Ch

Select Drives:

☑ Drive(SONY SDX-500C, Ser#0001481162@Scsi3:0,2,0)(FW:01e4)(\\.\Tap
☑ Drive(SONY SDX-500C, Ser#0001481170@Scsi3:0,1,0)(FW:01e4)(\\.\Tap

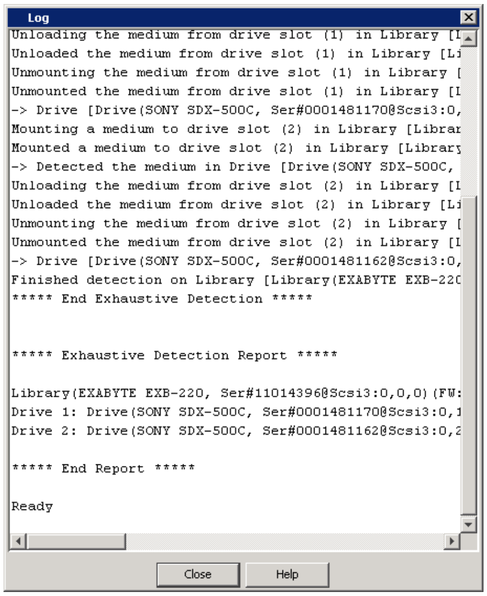
6. Optionally, from the **Processing** dialog box you can perform the following operations:
   - Click the **Abort** button to abort the exhaustive detection operation and unmount any mounted media from the drives.
   - Click the **View Log** button to display the **Log** dialog box which reports the status of each task that is performed during the exhaustive detection operation.



0%

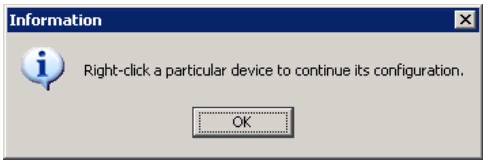
Elapsed Time: 00:00:00

7. When the exhaustive detection process is completed, the log file is displayed. Note the log file contents and click **Close** to proceed.



```
Unloading the medium from drive slot (1) in Library [L
Unloaded the medium from drive slot (1) in Library [Li
Unmounting the medium from drive slot (1) in Library [
Unmounted the medium from drive slot (1) in Library [L
-> Drive [Drive(SONY SDX-500C, Ser#0001481170@Scsi3:0,
Mounting a medium to drive slot (2) in Library [Librar
Mounted a medium to drive slot (2) in Library [Library
-> Detected the medium in Drive [Drive(SONY SDX-500C,
Unloading the medium from drive slot (2) in Library [L
Unloaded the medium from drive slot (2) in Library [Li
Unmounting the medium from drive slot (2) in Library [
Unmounted the medium from drive slot (2) in Library [L
-> Drive [Drive(SONY SDX-500C, Ser#0001481162@Scsi3:0,
Finished detection on Library [Library(EXABYTE EXB-220
***** End Exhaustive Detection *****


***** Exhaustive Detection Report *****

Library(EXABYTE EXB-220, Ser#11014396@Scsi3:0,0,0)(FW:
Drive 1: Drive(SONY SDX-500C, Ser#0001481170@Scsi3:0,1
Drive 2: Drive(SONY SDX-500C, Ser#0001481162@Scsi3:0,2

***** End Report *****

Ready
```

8. An **Information** prompt appears, informing you to right-click the device to continue the configuration. Click **OK** to proceed

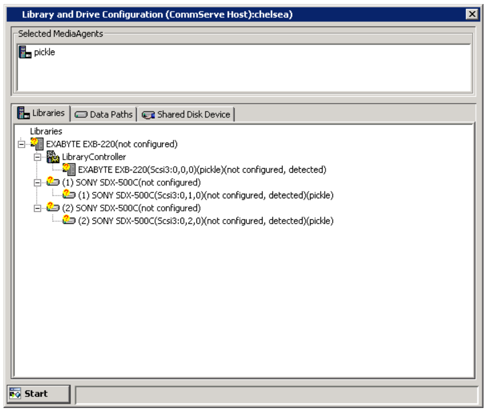


Right-click a particular device to continue its configuration.

Exhaustive detection may not be able to unload a drive, if it is not detected. If this occurs manually remove the media from the drive.

In the expanded tree in the sample image , the unconfigured devices controlled by MediaAgent are displayed.

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



```
Libraries
EXABYTE EXB-220(not configured)
  LibraryController
    EXABYTE EXB-220(Scsi3:0,0,0)(pickle)(not configured, detected)
  (1) SONY SDX-500C(not configured)
    (1) SONY SDX-500C(Scsi3:0,1,0)(not configured, detected)(pickle)
  (2) SONY SDX-500C(not configured)
    (2) SONY SDX-500C(Scsi3:0,2,0)(not configured, detected)(pickle)
```

9. Configure the library as described in Configure Devices.

DETECT DEVICES USING EXHAUSTIVE DETECTION ON A SPECIFIC LIBRARY/DRIVE/LIBRARY CONTROLLER

Required Capability: See Capabilities and Permitted Actions

BEFORE YOU BEGIN

- Review Exhaustive Detection.
- Verify that the necessary SCSI adapters and drivers for the library attached to the MediaAgent computer are installed.

  If you have two libraries with different drive types (e.g. AIT and DLT 4000 drive types) and even if you do not plan to use some of the drives, ensure that all the drivers associated with all the drives types are installed. In some cases, if you do not install all the appropriate drivers, the device configuration may fail.

  Consider the following:

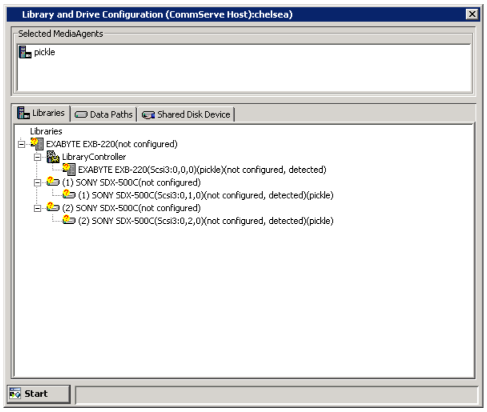
  - In a SAN environment you may have libraries with two different drive types connected to your bridge or switch (e.g., AIT and DLT 4000 drive types) If you planned on using only the DLT 4000 drives and hence only installed the drivers for the DLT 4000 drives, you would not be able to configure these drives in the **Library and Drive Configuration** window, until you install the drivers associated with all the other drive types (AIT) in the libraries.
  - If you have an existing library (e.g. a library with DLT 4000 drives) which is already configured, and if you add another library with another drive type into your environment (e.g. a library with AIT drives) the SCSI ID of the configured library may change and you may need to edit the address in the properties of the devices in the **Library and Drive Configuration** window.
- Check and verify that the hardware is visible to the operating system. For a more detailed explanation on verifying the driver configurations, see the following sections:
  - Hardware Configuration Guidelines - Direct-Attached Libraries
  - Hardware Configuration Guidelines - Direct-Attached Shared Library
  - Hardware Configuration Guidelines - Libraries Attached to a SAN
- Ensure that the CommServe computer and library are accessible.
- As this operation may involve the mounting of a media in a drive, ensure that media is available in the library. Also ensure that the media is not a cleaning media.
- Exhaustive detection should not be performed when other jobs are using the drives in the library. Stop all jobs before performing an exhaustive detection.
- Verify and ensure that no media is mounted in the drives available in the libraries connected to the selected MediaAgent(s).

CAUTION

Before configuring the libraries and drives in SAN, we strongly recommend you to verify and ensure that proper hardware zoning of tape drives be implemented, especially when you have HBA fail over implemented in your environment. For more information on zoning of HBA fail over, contact your HBA software vendor.

TO PERFORM AN EXHAUSTIVE DETECTION FOR THE LIBRARY/DRIVE/LIBRARY CONTROLLER

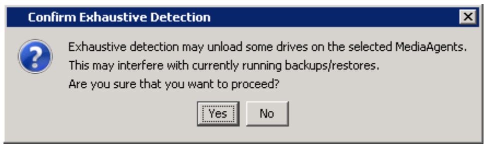
1. Display the Library and Drive Configuration window.
2. Right-click the Library, Drive or the Library Controller, select **Advanced Options** and click **Exhaustive Detection**.



pickle

Libraries
- EXABYTE EXB-220(not configured)
  - LibraryController
    - EXABYTE EXB-220(Scsi3:0,0,0)(pickle)(not configured, detected)
  - (1) SONY SDX-500C(not configured)
    - (1) SONY SDX-500C(Scsi3:0,1,0)(not configured, detected)(pickle)
  - (2) SONY SDX-500C(not configured)
    - (2) SONY SDX-500C(Scsi3:0,2,0)(not configured, detected)(pickle)

3. Click **Yes** to continue.

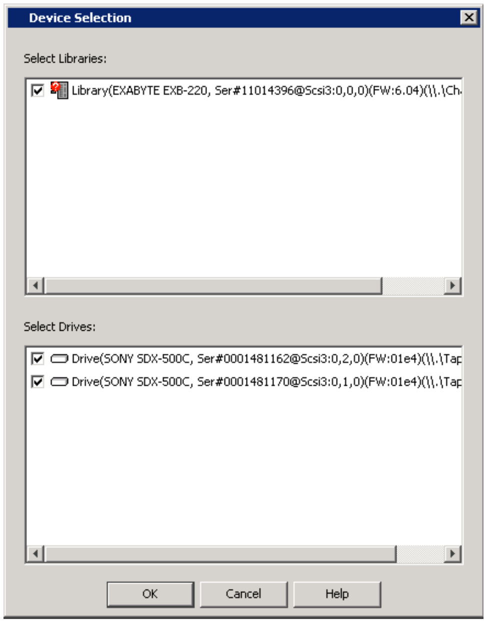


Exhaustive detection may unload some drives on the selected MediaAgents.
This may interfere with currently running backups/restores.
Are you sure that you want to proceed?

4. From the **Device Selection** dialog box, select the libraries and drives you wish to detect and then click **OK**.

   The detection process will attempt to detect the devices by mounting the media in each of the selected drives to determine the correct drive to library mapping.

   You can track the progress of the operation in the **Processing** dialog box.



Select Libraries:

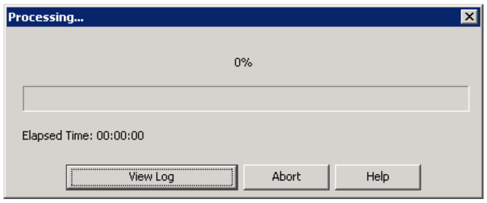
☑ Library(EXABYTE EXB-220, Ser#11014396@Scsi3:0,0,0)(FW:6.04)(\\.\Ch

Select Drives:

☑ Drive(SONY SDX-500C, Ser#0001481162@Scsi3:0,2,0)(FW:01e4)(\\.\Tap

☑ Drive(SONY SDX-500C, Ser#0001481170@Scsi3:0,1,0)(FW:01e4)(\\.\Tap

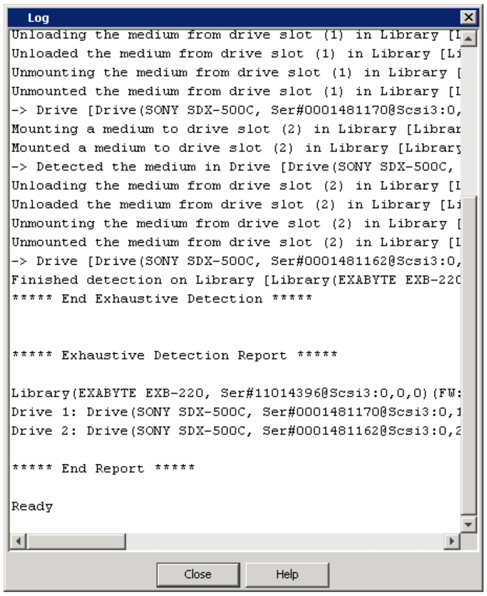
5. Optionally, from the **Processing** dialog box you can perform the following operations:
   - Click the **Abort** button to abort the exhaustive detection operation and unmount any mounted media from the drives.
   - Click the **View Log** button to display the **Log** dialog box which reports the status of each task that is performed during the exhaustive detection operation.



0%

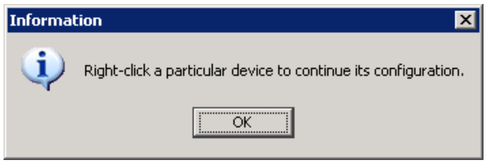
Elapsed Time: 00:00:00

6. When the exhaustive detection process is completed, the log file is displayed. Note the log file contents and click **Close** to proceed.



```
Unloading the medium from drive slot (1) in Library [I
Unloaded the medium from drive slot (1) in Library [Li
Unmounting the medium from drive slot (1) in Library [
Unmounted the medium from drive slot (1) in Library [I
-> Drive [Drive(SONY SDX-500C, Ser#0001481170@Scsi3:0,
Mounting a medium to drive slot (2) in Library [Librar
Mounted a medium to drive slot (2) in Library [Library
-> Detected the medium in Drive [Drive(SONY SDX-500C,
Unloading the medium from drive slot (2) in Library [I
Unloaded the medium from drive slot (2) in Library [Li
Unmounting the medium from drive slot (2) in Library [
Unmounted the medium from drive slot (2) in Library [I
-> Drive [Drive(SONY SDX-500C, Ser#0001481162@Scsi3:0,
Finished detection on Library [Library(EXABYTE EXB-220
***** End Exhaustive Detection *****


***** Exhaustive Detection Report *****

Library(EXABYTE EXB-220, Ser#11014396@Scsi3:0,0,0)(FW:
Drive 1: Drive(SONY SDX-500C, Ser#0001481170@Scsi3:0,1
Drive 2: Drive(SONY SDX-500C, Ser#0001481162@Scsi3:0,2

***** End Report *****

Ready
```

7. An **Information** prompt appears, informing you to right-click the device to continue the configuration. Click **OK** to proceed

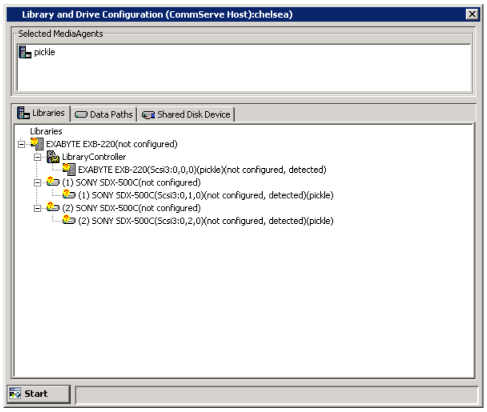


Right-click a particular device to continue its configuration.

Exhaustive detection may not be able to unload a drive, if it is not detected. If this occurs manually remove the media from the drive.

In the expanded tree in the sample image, the unconfigured devices controlled by MediaAgent are displayed.

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



```
Libraries
EXABYTE EXB-220(not configured)
    LibraryController
        EXABYTE EXB-220(Scsi3:0,0,0)(pickle)(not configured, detected)
    (1) SONY SDX-500C(not configured)
        (1) SONY SDX-500C(Scsi3:0,1,0)(not configured, detected)(pickle)
    (2) SONY SDX-500C(not configured)
        (2) SONY SDX-500C(Scsi3:0,2,0)(not configured, detected)(pickle)
```

8. Configure the library as described in Configure Devices.

CONFIGURE DEVICES

Related Topics

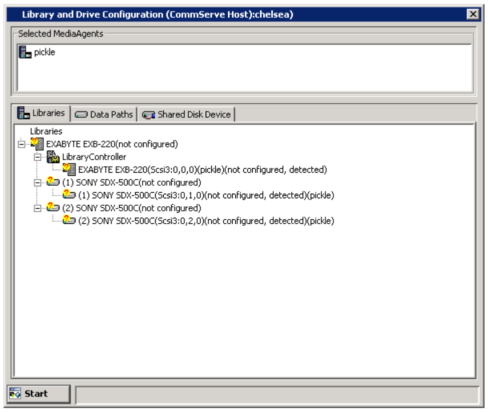
- Configuration

The following procedure describes the steps involved in configuring devices attached to a MediaAgent or NAS File Server.

TO CONFIGURE A LIBRARY

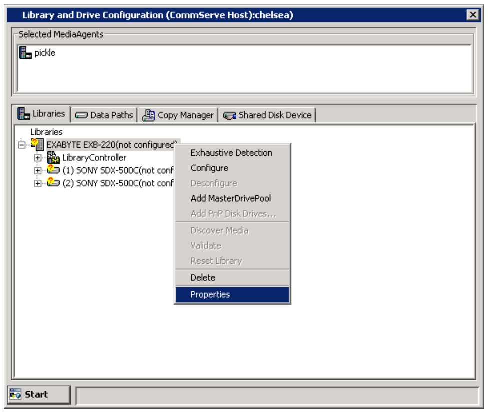
1. Display the Library and Drive Configuration window.
2. Detect the devices. Use Detection or Exhaustive Detection as required.

   Note that the **Library and Drive Configuration** window displays a master drive pool (with a drive pool and the associated drives) for the library.


Library and Drive Configuration (CommServe Host):chelsea)
Selected MediaAgents
pickle
Libraries
Data Paths
Shared Disk Device
Libraries
EXABYTE EXB-220(not configured)
LibraryController
EXABYTE EXB-220(Scsi3:0,0,0)(pickle)(not configured, detected)
(1) SONY SDX-500C(not configured)
(1) SONY SDX-500C(Scsi3:0,1,0)(not configured, detected)(pickle)
(2) SONY SDX-500C(not configured)
(2) SONY SDX-500C(Scsi3:0,2,0)(not configured, detected)(pickle)
Start

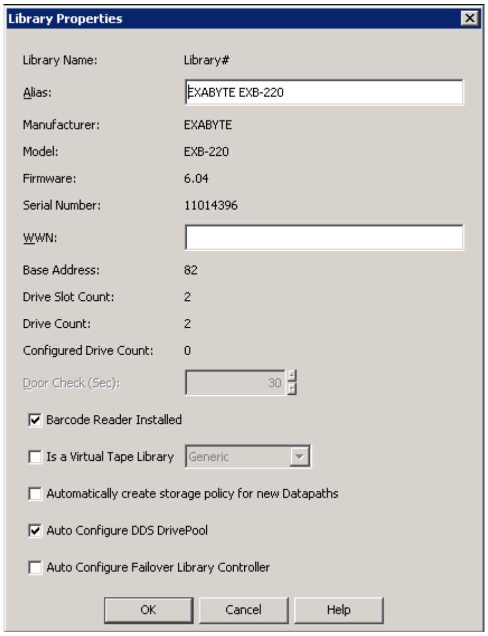
3. Optionally, perform the following steps if you do not want the system to automatically create a storage policy during configuration:

   Right-click the library and then click **Properties**.



   From the **Library Properties** window, if necessary, clear the **Automatically create storage policy for new Datapaths** option.

   Click **OK**.



Library Properties

Library Name: Library#

Alias: EXABYTE EXB-220

Manufacturer: EXABYTE

Model: EXB-220

Firmware: 6.04

Serial Number: 11014396

WWN:

Base Address: 82

Drive Slot Count: 2

Drive Count: 2

Configured Drive Count: 0

Door Check (Sec): 30

☑ Barcode Reader Installed

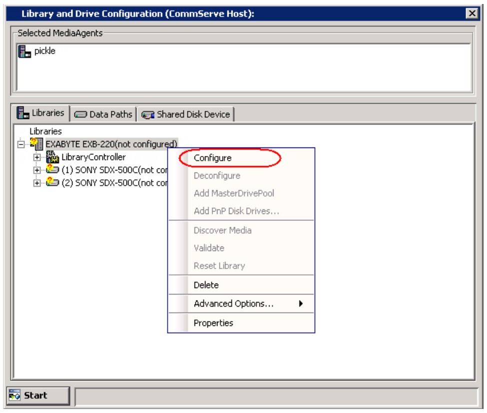
☐ Is a Virtual Tape Library Generic

☐ Automatically create storage policy for new Datapaths

☑ Auto Configure DDS DrivePool

☐ Auto Configure Failover Library Controller

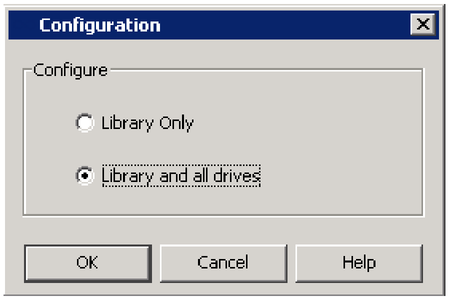
4. From the **Library and Drive Configuration** window, right-click the library that you want to configure, and then click **Configure**.


Library and Drive Configuration (CommServe Host):

Selected MediaAgents: pickle

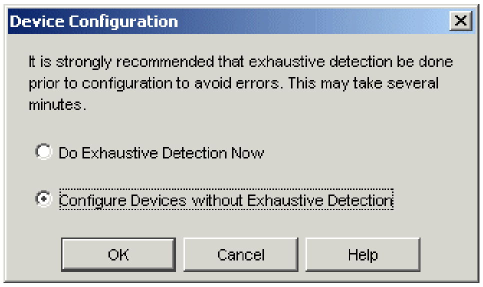
Libraries
- EXABYTE EXB-220(not configured)
  - LibraryController
  - (1) SONY SDX-500C(not co
  - (2) SONY SDX-500C(not co

5. Choose one of the following options from the **Configuration** dialog box:
   - **Library only** option if you want to configure the drives individually. (See Configuring a Drive for information on individually configuring the drives.)
   - **Library and all drives** option if you want to configure all the drives within the library (e.g., if you are doing a typical library installation)


Configuration

Configure
- ○ Library Only
- ● Library and all drives

6. If you have not already performed an exhaustive detection, or if your exhaustive detection did not detect one or more of the existing devices, the **Device Configuration** dialog box is displayed. Choose one of the following options:
   - Choose the **Do Exhaustive Detection Now** option if you wish to perform the exhaustive detection operation. If you choose this option, follow steps 5 to 8 in the procedure, Detect Devices Using Exhaustive Detection.
   - Choose the **Configure Devices without Exhaustive Detection** option if you do not wish to perform the exhaustive detection operation.


Device Configuration

It is strongly recommended that exhaustive detection be done prior to configuration to avoid errors. This may take several minutes.

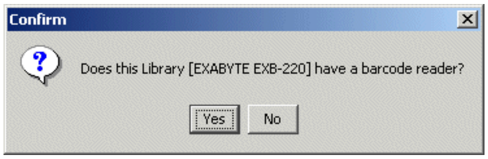
- ○ Do Exhaustive Detection Now
- ● Configure Devices without Exhaustive Detection

7. A **Confirm** prompt appears, asking you if your library has a barcode reader.
   - Click **Yes**, if the library has a barcode reader. (sighted library)
   - Click **No**, if the library does not have a barcode reader. (blind library)

   On Windows MediaAgents, this prompt is displayed only in the following situations:

   - When the media changer is disabled in the operating system.
   - When the media changer is enabled, but the operating system detects an unknown media changer.

   If Windows detects the correct media changer, this prompt will *not* be displayed.


Confirm

Does this Library [EXABYTE EXB-220] have a barcode reader?

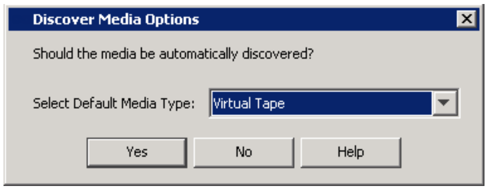
8. If the library has a barcode reader, the **Discover Media Options** dialog box is displayed.

   Perform one of the following:

   - To automatically discover the media in the library, select the default media type and then click **Yes**.
   - To manually discover the media, click **No**.

   For more information on discovering media in a library, see Discover Media.

   Ensure that media is discovered, before using the library for a data protection operations.

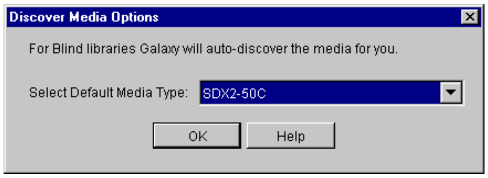

Discover Media Options

Should the media be automatically discovered?

Select Default Media Type: Virtual Tape

9. If the library does not have a barcode reader, the **Discover Media Options** dialog box is displayed.

   Select the correct media type available in the library and then click **OK**.



For Blind libraries Galaxy will auto-discover the media for you.

Select Default Media Type: SDX2-50C

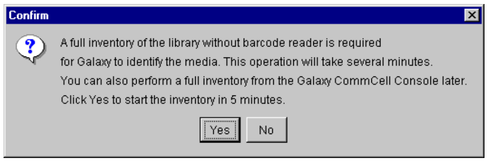
10. If the library does not have a barcode reader the **Confirm** prompt is displayed.
    - Click **Yes**, if you want to automatically start the inventory process after 5 minutes.
    - Click **No**, if you want to manually start the inventory process. Ensure that a full inventory is performed on the library, before using the library for a data protection operations.

    For libraries without a barcode reader, read the information provided in Blind Library Configuration.

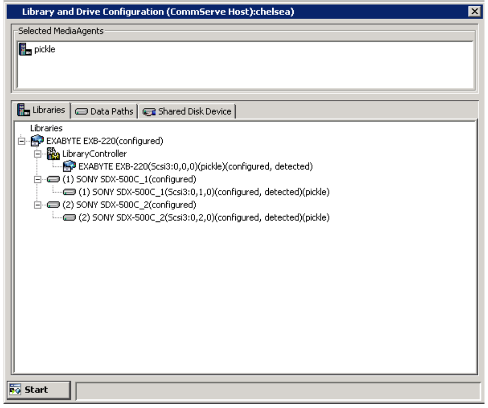
    The status of the library changes to **configured**. If you chose to configure all associated drives, the status of the drives (and of the drive pool that contains them) changes to **configured** as well.

    If the library is an optical library, the system automatically identifies the optical library and uses the optical library icon to display the library information.

    The **Library** tab provides the physical view of the devices (library and drives).

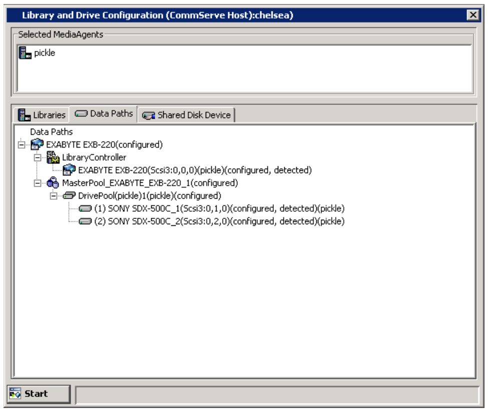


A full inventory of the library without barcode reader is required
for Galaxy to identify the media. This operation will take several minutes.
You can also perform a full inventory from the Galaxy CommCell Console later.
Click Yes to start the inventory in 5 minutes.



```
pickle

Libraries
⊟ EXABYTE EXB-220(configured)
   ⊟ LibraryController
      EXABYTE EXB-220(Scsi3:0,0,0)(pickle)(configured, detected)
   ⊟ (1) SONY SDX-500C_1(configured)
      (1) SONY SDX-500C_1(Scsi3:0,1,0)(configured, detected)(pickle)
   ⊟ (2) SONY SDX-500C_2(configured)
      (2) SONY SDX-500C_2(Scsi3:0,2,0)(configured, detected)(pickle)
```

The **Data Paths** tab provides a logical view of the data path used to access the devices - library, master drive pool, drive pool, drive.



```
pickle

Data Paths
⊟ EXABYTE EXB-220(configured)
   ⊟ LibraryController
      EXABYTE EXB-220(Scsi3:0,0,0)(pickle)(configured, detected)
   ⊟ MasterPool_EXABYTE_EXB-220_1(configured)
      ⊟ DrivePool(pickle)1(pickle)(configured)
         (1) SONY SDX-500C_1(Scsi3:0,1,0)(configured, detected)(pickle)
         (2) SONY SDX-500C_2(Scsi3:0,2,0)(configured, detected)(pickle)
```

VALIDATE THE DRIVES IN A LIBRARY

The following procedure describes the steps for validating drives in a library.

BEFORE YOU BEGIN:

- You should have discovered at least one new media before attempting to validate a drive
- Validation of drives cannot be performed if media is in the drives. Therefore, do not validate the devices until you remove the media from the drives.
- Do not validate drives when a job is in progress in the library.
- Do not run any jobs when you validate drives. Disable all scheduled jobs in the library you wish to validate. You can do this by disabling the jobs in the Activity Control dialog box at the appropriate level in the CommServe tree.
- Drive validation may fail because of a mount or unmount problem. For an unmount error, unload the media manually and **Reset** the library.

Required Capability: See Capabilities and Permitted Actions

To validate the SCSI mapping of drives within a library:

1. Display the Library and Drive Configuration window.

2. Right-click the configured library, master drive pool, drive pool or drive that you want to validate, and then click **Validate**. Note that the library must contain discovered media. (For information on discovering media, see Discover Media from the CommCell Console.)
3. A prompt appears, informing you that validation may take several minutes per drive and asking if you want to continue. Click **Yes** to start the validation process.

   The system attempts to mount a media in each drive within the library, master drive pool, drive pool or drive. A progress bar reports the progress of the validation job.

   Click on the **View Log** button to display the **Log** dialog box which reports the status of each task that is performed during the drive validation operation.

   A status message reporting the success or failure of the operation appears in the Status Bar at the bottom of the `Library and Drive Configuration` window.

CHANGE THE LIBRARY NAME

Required Capability: See Capabilities and Permitted Actions

To change the library name:

1. Display the Library and Drive Configuration window.
2. Right-click the library for which you wish to change the name, and then click **Properties**.
3. In the **Alias** box, type the new name for the library.
4. Click **OK** to save the changes.

CHANGE THE DOOR CHECK SECONDS FOR A LIBRARY

Required Capability: See Capabilities and Permitted Actions

To change the door check seconds for a library:

1. Display the Library and Drive Configuration window.
2. Right-click the library for which you wish to change the door check seconds, and then click **Properties**.
3. In the **Door Check (sec)** box, type or select the frequency (in seconds) that the library door is checked to be open.
4. Click **OK** to save the changes.

ENABLE AUTOMATIC MEDIA DISCOVERY DURING LIBRARY CONFIGURATION

Required Capability: Capabilities and Permitted Actions

To discover media within a library:

1. Display the Library and Drive Configuration window.
2. Detect the devices. Use Detection or Exhaustive Detection as required.
3. Configure the library as described in Configure Devices.

   During the configuration process, if the library has a barcode reader, the **Discover Media Options** dialog box is displayed.

   Perform one of the following:

   - To automatically discover the media in the library, select the default media type and then click **Yes**.
   - To manually discover the media, click **No**. See Discover Media from the CommCell Console for step-by-step instructions on manually discovering media in a library.

     Ensure that media is discovered, before using the library for a data protection operations.

   If the library does not have a barcode reader, another **Discover Media Options** dialog box is displayed.

   Select the correct media type available in the library and then click **OK**.

CONFIGURING LIBRARY FOR SOLARIS ZONES

You can configure a library or a device in a global zone and then access the same library from a local zone. Use the SCSiZone tool to configure the library in the global zone. Follow the steps given below to configure the library:

1. Install the MediaAgent on the computer hosting the global zone. For more information, refer to Install the MediaAgent - Solaris.

2. Install the MediaAgent on the local zone. For more information, refer to Install the MediaAgent - Solaris.

3.
   - On the computer hosting the global zone, navigate to `the` following location:

     ```
     <Install Directory>/WA
     ```

   - Enter the following command to detect the devices:

     ```
     ./wa_sunqlc_add
     ```

   The library and tape drive devices are detected. To confirm this, navigate to to `/var/adm/` and view the messages file. It displays the list of detected devices.

4. On the local zone, enter the following command to stop the Calypso services:

   ```
   simpana stop
   ```

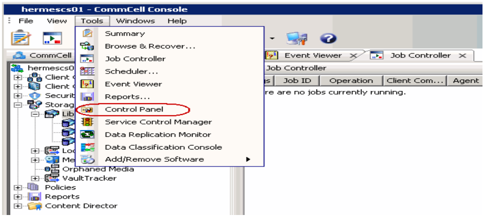
5. On the global zone, navigate to `<Install Directory>/Base` and enter the following command:

   ```
   ./ScsiZoneTool -i <local zone name>
   ```

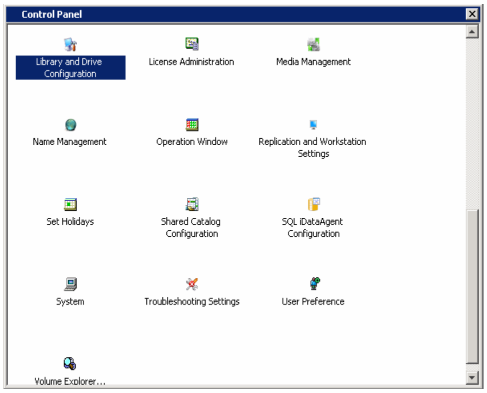
6. Restart the services on the local zone using the following commnad:

   ```
   simpana start
   ```

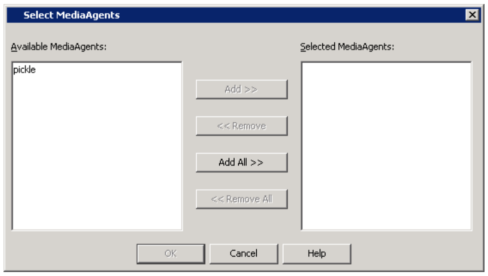
7. From the **Tools** menu in the CommCell Console, click **Control Panel**.



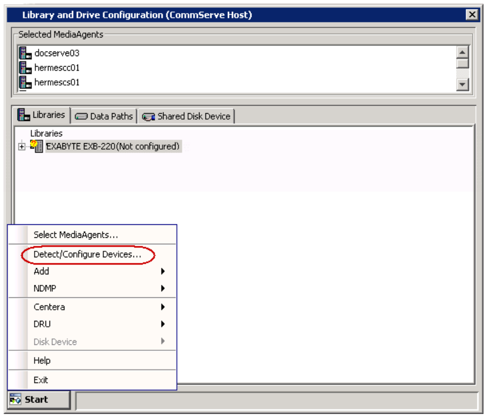
8. Double click **Library & Drive Configuration**.



9.
   - Select the MediaAgent(s) installed on the local Zone.
   - Click **OK**.

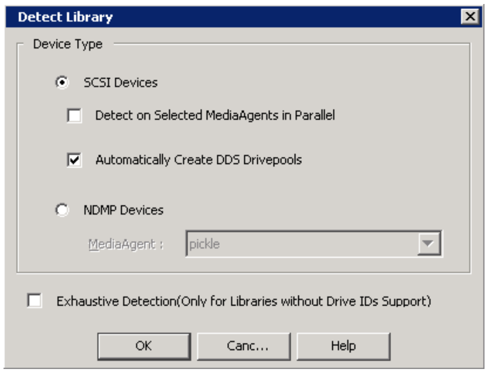


10. From the **Library and Drive Configuration** window, click the **Start** menu and choose **Detect/Config Devices**.



11. In the **Detect Library** dialog box, select **SCSI Devices**.

    Click **OK**.



Detect Library

Device Type

● SCSI Devices

☐ Detect on Selected MediaAgents in Parallel

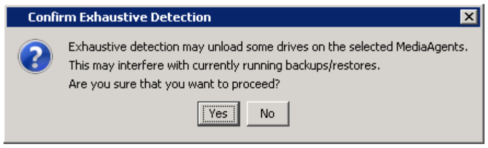
☑ Automatically Create DDS Drivepools

○ NDMP Devices

MediaAgent : pickle

☐ Exhaustive Detection(Only for Libraries without Drive IDs Support)

12. Click **Yes** to continue.



Confirm Exhaustive Detection

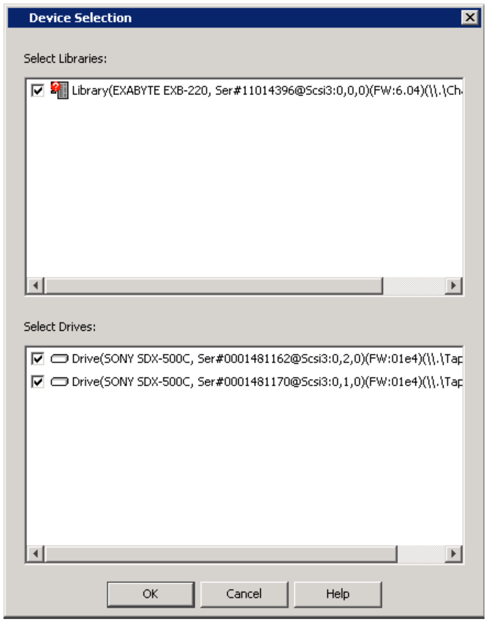
Exhaustive detection may unload some drives on the selected MediaAgents. This may interfere with currently running backups/restores. Are you sure that you want to proceed?

13. From the **Device Selection** dialog box, select the libraries and drives you wish to detect and then click **OK**.

    This dialog box displays the same list of library and tape drives that appeared on global zone.

    The detection process will attempt to detect the devices by mounting the media in each of the selected drives to determine the correct drive to library mapping.

    You can track the progress of the operation in the **Processing** dialog box.



Device Selection

Select Libraries:

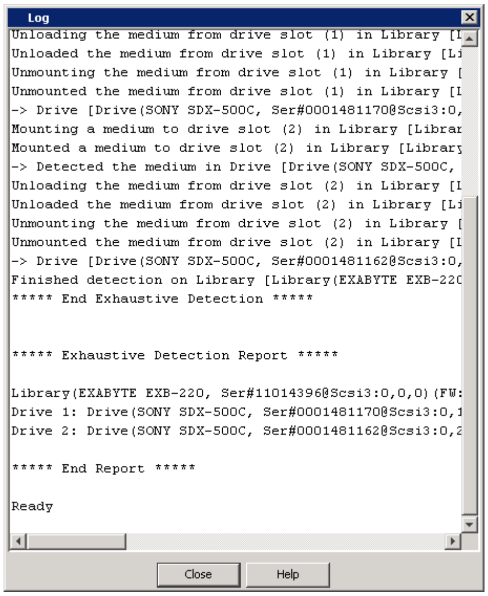
☑ Library(EXABYTE EXB-220, Ser#11014396@Scsi3:0,0,0)(FW:6.04)(\\.\Ch

Select Drives:

☑ Drive(SONY SDX-500C, Ser#0001481162@Scsi3:0,2,0)(FW:01e4)(\\.\Tap

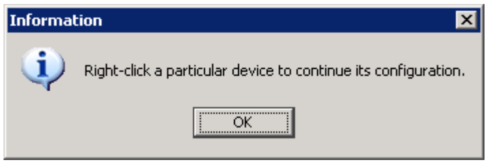
☑ Drive(SONY SDX-500C, Ser#0001481170@Scsi3:0,1,0)(FW:01e4)(\\.\Tap

14. When the exhaustive detection process is completed, the log file is displayed. Note the log file contents and click **Close** to proceed.



```
Unloading the medium from drive slot (1) in Library [L
Unloaded the medium from drive slot (1) in Library [Li
Unmounting the medium from drive slot (1) in Library [
Unmounted the medium from drive slot (1) in Library [L
-> Drive [Drive(SONY SDX-500C, Ser#0001481170@Scsi3:0,
Mounting a medium to drive slot (2) in Library [Librar
Mounted a medium to drive slot (2) in Library [Library
-> Detected the medium in Drive [Drive(SONY SDX-500C,
Unloading the medium from drive slot (2) in Library [L
Unloaded the medium from drive slot (2) in Library [Li
Unmounting the medium from drive slot (2) in Library [
Unmounted the medium from drive slot (2) in Library [L
-> Drive [Drive(SONY SDX-500C, Ser#0001481162@Scsi3:0,
Finished detection on Library [Library(EXABYTE EXB-220
***** End Exhaustive Detection *****


***** Exhaustive Detection Report *****

Library(EXABYTE EXB-220, Ser#11014396@Scsi3:0,0,0)(FW:
Drive 1: Drive(SONY SDX-500C, Ser#0001481170@Scsi3:0,1
Drive 2: Drive(SONY SDX-500C, Ser#0001481162@Scsi3:0,2

***** End Report *****

Ready
```

15. An **Information** prompt appears, informing you to right-click the device to continue the configuration. Click **OK** to proceed.



Right-click a particular device to continue its configuration.

16. Configure the library as described in Configure Devices.

Blind Libraries

Topics | Configure | How To | Related Topics

OVERVIEW

A *blind* library is a library without a barcode reader, and is the opposite of a *sighted* library which has a barcode reader.

Blind libraries can be configured using the **Library and Drive Configuration** window. During any library configuration the configuration process displays a prompt to confirm the presence or absence of a barcode reader in the library. If you indicate that the library does not contain a barcode reader, the library will be configured as a blind library. A blind library must have all its drives (and media) of the same type.

Once configured, a blind library cannot be converted as a sighted library.

Blind libraries have two distinctive features used by the MediaAgent software to identify media in the absence of a barcode reader. They are:

- **Library Inventory**

  The MediaAgent software manages the media within a library by performing several types of inventory jobs to keep track of the slot numbers or drives in which the media are stored or mounted. For a detailed explanation of the inventory operation in a blind library, see Inventory Operations in Blind Libraries.

- **On Media Label (OML)**

  Each media is initialized by writing an OML on the media when it is first mounted during the inventory/discover process. When the media is accessed later, the OML is used to validate and ensure that the correct media is mounted on the drive. (Note that for spare media in a sighted library, the new OML will not be created until the data is about to be written for the first time.)

  Note that the OML will be written on both sides for an optical media.

BLIND LIBRARY OPERATIONS

Most of the operations in a blind library are similar to the operations in a sighted library. The operations that are specific to the blind library are described in the following sections. For information on operations that are similar in both sighted and blind libraries, see Library Operations.

The following table lists the operations in the blind and sighted library.

OPTIONS	BLIND LIBRARY	SIGHTED LIBRARY	ADDITIONAL INFORMATION
New Scratch Pool	X	X	See Library Operations
Verify Media	X	X	See Verifying Media in Blind Libraries
Discover Media	X	X	See Discovering Media in Blind Libraries

Import Media	X	X	See Importing Media into Blind Libraries
Export Media (with Verify option)	X	X	See Exporting Media from Blind Libraries
Reset Library	X	X	See Library Operations
Mark Library Fixed	X	X	See Library Operations
Mark Media Exported	X	X	See Library Operations
Inventory	X		See Inventory Operations in Blind Libraries

AUDIT TRAIL

Operations performed with this feature are recorded in the Audit Trail. See Audit Trail for more information.

INVENTORY OPERATIONS IN BLIND LIBRARIES

Several types of inventory operations in a blind library is used to identify, discover and search all or certain media in the blind library and to ensure that the slot occupancy and media identity are correctly associated in the CommServe database. The following inventory operations are performed in a blind library:

- Full Inventory
- Quick Inventory
- Search Inventory

The above inventory operations are displayed as a job in the **Job Controller** window and can be killed if necessary. Information pertaining to the media discovered prior to the killing of the full inventory operation will be retained.

The system, by default uses all the drives in the library to perform the inventory operation. Similarly, the system tries to reserve drives for performing inventory operation, every 120 seconds.

For step-by-step instructions, see Perform an Inventory Operation in a Blind Library.

FULL INVENTORY

The full inventory operation may be initiated or scheduled by the user. The full inventory operation is used to identify the media used by the CommCell, initialize any new media, to prepare and update the media list in the library and to keep track of the location of the media within the library.

During a full inventory process, each of the media available in the library is mounted to read the OML.

- If a valid OML is found, the media information will be associated with the slot occupied and updated in the CommServe database.
- If a valid OML is not found, a new OML may or may not be created, subject to the criteria established for overwriting media in the library. For more information on the criteria for overwriting media, see the details for the Overwrite Media option available in **Library Properties** dialog box.

The full inventory operation may take several minutes, depending on the number of drives and the media available in the library. You must initiate a full inventory operation as soon as you configure a blind library and before you use the library for a data protection operation. You may perform a **Full Scan** of the library when you initiate a full inventory operation on the blind library. (See Full Scan for a detailed explanation on the full scan option.)

A full inventory operation is run with the lowest job priority, which means that it does not interfere with or interrupt other jobs that use the library. However, it is recommended that you run a full inventory operation when other jobs are not running or scheduled to occur. This ensures that the inventory operation utilizes all the available resources and completes the operation in the least amount of time.

A full inventory job can be scheduled and history information about the inventory can be viewed from the Admin Job History window.

QUICK INVENTORY

The quick inventory operation must be initiated or scheduled by the user. A quick inventory operation is similar to a Full Inventory operation but is performed on only the newly occupied slots. Hence the quick inventory can be performed when you import new media into the library. (You may perform a **Full Scan** of the library when you initiate a quick inventory operation, (See Full Scan for a detailed explanation on the full scan option.)

During the quick inventory process, the system mounts the media from the newly occupied slots and attempts to read the OML on the media.

- If a valid OML is found, the media information will be associated with the slot occupied and updated in the CommServe database.
- If a valid OML is not found, new OML is created.

A quick inventory operation is run with the lowest job priority, which means that it does not interfere with or interrupt other jobs that use the library.

SEARCH INVENTORY

When a job requests a specific media and if the media is not found in the original slot stored in the CommServe database, a search inventory operation will be initiated in the library to locate the media. The search inventory operation attempts to locate the media, by mounting and reading the OML from media in slot locations which were unknown or not confident. The search operation continues until the media is found. During a search inventory operation, new media will be initialized as in a Full or Quick inventory operation.

A search inventory operation is run with the highest job priority, which means that it will interrupt all **Restartable** jobs that use the library.

FULL SCAN

The full scan option must be used along with an inventory to check the media occupancy in the library slots and update the slot table in the CommServe database.

A full scan operation is recommended in the following situations:

- When you export or import media directly through the library's mail slot or when you open the library door and manually add or remove media or rearrange the media in the storage slots.

  It is therefore recommended that you initiate a full scan when ever you import/export media into a library, especially libraries without a mail slot.
- When a Quick inventory operation fails to detect new media.

The library status is displayed as *offline* until the full scan operation completes. This means that new data protection or data recovery operations that access the library cannot start until the operation completes. A data protection or data recovery operation that is in progress when the full scan operation begins can continue as long as it does not need to access unmounted media.

VERIFYING MEDIA IN BLIND LIBRARIES

The verify media operation is a type of inventory which must be initiated by the user. This operation can be used to verify whether the media information displayed in the CommCell Console matches the OML in the media. There are two ways to initiate a verify inventory operation:

- You can right-click a media and then choose the Verify Media option.
- You can select the Verify Media option when you export the media or schedule an export (both from a list or based on a criteria). This option may be used to verify that the correct media is exported.

A verify inventory operation is displayed as a job in the **Job Controller** window and can be **Killed** if necessary. The verify inventory operation does not discover new media.

For step-by-step instructions, see Verify Media in a Blind Library.

DISCOVERING MEDIA IN BLIND LIBRARIES

Discover media is the process by which the MediaAgent software initializes new media and stores the media information in the CommServe database.

In a blind library the discover media operation is available only at the media level.

The discover media operation mounts the media into a drive and if a valid OML is not found, it writes the OML on the media. Once unmounted, the system also keeps track of the media location.

A discover inventory job is displayed in the **Job Controller** window and can be **Killed** if necessary. Also note that both the full and quick inventory processes will automatically discover new media whenever a new media is found.

For step-by-step instructions, see Discover Media in a Blind Library.

IMPORTING MEDIA INTO BLIND LIBRARIES

Importing is the process by which you move media that are outside a library into storage slots within the library. The import media operation in a blind library is similar to that of an import media operation in a sighted library. (For a detailed explanation on importing media, see Import Media.)

However, when you import media in a blind library, ensure that you perform a quick inventory with a full scan, in order to discover the imported media.

It is recommended that you initiate a full scan operation (if it is not automatically triggered) whenever you directly import media into a library, especially on libraries without a mail slot.

For step-by-step instructions, see Import Media Into a Blind Library.

EXPORTING MEDIA FROM BLIND LIBRARIES

Exporting is the process by which you physically remove one or more media from a library. The export media operation in a blind library is similar to that of an export media operation in a sighted library. (For a detailed explanation on exporting media, see Export Media.)

However, when you export media in a blind library, an option to verify the media is displayed, to ensure that the correct media is exported. Media that fails verification will not be exported. The media verification operation is not performed when the export media operation is scheduled.

When media is exported immediately from a blind library (not a scheduled export operation) the media export job is displayed in the **Job Controller** window and can be **Killed** if necessary.

It is recommended that you initiate a quick inventory with full scan operation (if it is not automatically triggered) when ever you directly export media from a library, especially on libraries without a mail slot.

MEDIA LABELING IN BLIND LIBRARIES

AUTOMATIC LABELING SCHEMES

The MediaAgent provides the facility to automate the process of labeling media (On Media Label - OML) in blind libraries. Several Labeling Options are provided to suit the labeling conventions used in your organization.

Care must be exercised while generating the labeling scheme to ensure that each media label is unique. If the specified labeling scheme is not unique, and if duplicate labels are found, the system automatically appends a media ID to make it unique.

SETTING-UP AUTOMATIC LABELING SCHEMES

Use the following steps to setup the media labeling scheme in blind libraries:

1. Specify the labeling scheme for a blind library, from the appropriate **Library Properties (Media)** tab. (For step-by-step instructions, see Create Automatic Labeling Schemes.)
2. The system will automatically stamp the label whenever a media inventory is performed.

MANAGING CLEANING MEDIA IN BLIND LIBRARIES

Cleaning media is automatically identified and moved to the **Cleaning Media Pool** when a full or quick inventory is performed.

However keep in mind that the cleaning media does not contain an OML and hence the system cannot differentiate each cleaning media, if multiple cleaning media are present. The cleaning media may get mounted whenever a full inventory operation is initiated which may result in the drive getting cleaned and the counters for drive cleaning reset.

For this reason we recommend the following:

- Do not store the cleaning media in a blind library
- Manually initiate the drive cleaning operation whenever it is required, using one of the following methods:
  - Using the menu options in the library front panel. In such a situation you, you must indicate to the MediaAgent that the drive has been cleaned as described in Resetting Counters When Drives are Cleaned using Library Options.
  - Import the Cleaning Media as described in Importing Cleaning Media. Clean the drive as described in Manually Initiating a Drive Cleaning Operation using the CommCell Console. Once the cleaning operation is completed export the cleaning media from the library, as described in Exporting a Specific Media.

BEST PRACTICES FOR BLIND LIBRARIES

Observe the follow guideline while using a blind library:

- Do not operate the library manually while an inventory operation is in progress.
- Always request a full or quick inventory with full scan after you manually rearrange the media between the library slots or add or remove media directly (without exporting it first) from a blind library.
- Perform a **Quick Inventory** with **Full Scan** whenever you import media into a library.
- From the Media tab of the **Library Properties** associated with blind libraries, under the Start New Media pane, ensure that the **When required media is exported** option is enabled.
- As inventory and verify media operations have a lower job priority, make sure that at least one drive is free when these operations are initiated, especially when you need to import media for an active job.
- Do not store cleaning media in a blind library. Import the cleaning media when it is required and export it after using it.
- Label all the exported media for future identification.

- Remove all the failed-to-be inventoried media, (i.e., bad, wrong format, write protected, etc.) from the library.

Back To Top

Blind Libraries - Configure

Topics | Configure | How To | Related Topics

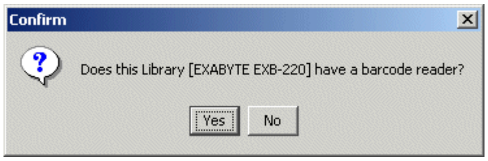
A blind library can be configured using one of the following configurations:

- Direct-attached library (See Configure a Direct-Attached Library with Similar Drive Types for more information.)
- Direct-attached shared library. (See Configure a Direct-Attached Shared Library for more information.)

In either of the above-mentioned configurations, ensure that you perform the following tasks during a blind library configuration process:

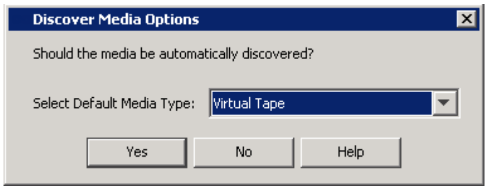
Select the correct button to indicate that the library does not contain a barcode reader. This can be done as follows:

- Click **No** in the **Confirm** prompt asking you whether the library has a barcode reader.



Does this Library [EXABYTE EXB-220] have a barcode reader?

In addition make sure that the correct media type used in the library is selected in the following **Discover Media Options** dialog box.

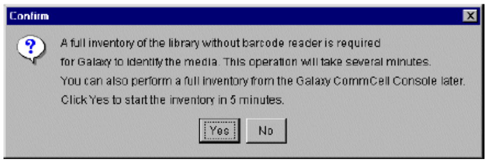


Should the media be automatically discovered?

Select Default Media Type: Virtual Tape

Also ensure that a full inventory is performed on the library. This can be done using either one of the following options:

- During the configuration, select **Yes** in the **Confirm** prompt asking you whether an inventory operation can be automatically performed after five minutes.



A full inventory of the library without barcode reader is required for Galaxy to identify the media. This operation will take several minutes. You can also perform a full inventory from the Galaxy CommCell Console later. Click Yes to start the inventory in 5 minutes.

From the **CommCell Console**, right-click the blind library for which you wish to perform an inventory. and then click **Inventory**.

From the **Inventory Options** dialog box, choose **Full Inventory**, check **Do Full Scan** and then click **OK**.

Blind Libraries - How To

Topics | Configure | How To | Related Topics

Import Media Into a Blind Library

Required Capability: See Capabilities and Permitted Actions

To import media into a blind library:

1. From the CommCell Browser, right-click the library (or the scratch pool of the library) into which you want to import media, and then click **Import Media**.
2. An Import Media prompt appears, advising you to do one of the following:
   - If you are importing through a mail slot, insert one or more media into the mail slot and wait for them to be moved to storage slots. Do not click **OK**

until all of the imported media have been moved to storage slots.

After all media are transferred to storage slots, click **OK** in the Import Media prompt.

- If you are inserting media directly, open the library door, insert media into storage slots, and then close the door.

  Wait for the library to complete the inventory and then click **OK** in the Import Media prompt.

3. A **Confirm Dialog** prompt asks you whether you wish to perform a quick scan.
   - Click **Yes** to perform a Quick Scan on the library. You can track the progress of the scan operation in the **Job Controller**.
   - Click No if you do not wish to perform a quick scan. To discover the media, you must perform either one of the following:
     - A Quick Inventory with Full Scan. For more information, see Perform an Inventory Operation in a Blind Library.
     - Individually discover each of the media you imported. For more information, see Discover Media in a Blind Library.

DISCOVER MEDIA IN A BLIND LIBRARY

Required Capability: See Capabilities and Permitted Actions

To discover media in a blind library:

1. From the CommCell Console, right-click the media you wish to discover and then click **Discover Media**.

   The system attempts to discover the media and reports the success or failure of the operation in the **Event Viewer**.

   Note that the discover operation is displayed as an inventory job in the **Job Controller** window.

PERFORM AN INVENTORY OPERATION IN A BLIND LIBRARY

Required Capability: See Capabilities and Permitted Actions

To perform an inventory in a blind library:

1. From the CommCell Console, right-click the blind library for which you wish to perform an inventory and then click **Inventory**.
2. From the Inventory Options dialog box, choose the type of inventory you wish to perform.
3. Select the **Do Full Scan** option if you want the inventory operation to scan all the library slots.
4. Click **OK**.

   You can track the progress of the inventory in the Job Controller window.

VERIFY MEDIA IN A BLIND LIBRARY

The verify media operation is a type of inventory which must be initiated by the user. There are two ways to initiate a verify inventory operation:

- You can right-click a media and then choose the **Verify Media** option. This operation can be used to verify whether the media information displayed in the CommCell Console matches the OML in the media.
- You can select the **Verify Media** option when you export the media or schedule an export (both from a list or based on a criteria). This option may be used to verify that the correct media is exported.

A verify inventory operation is displayed as a job in the **Job Controller** window and can be **killed** if necessary.

The verify inventory operation does not discover new media.

CONVERT A BLIND LIBRARY AS A SIGHTED LIBRARY

To convert a blind library as a sighted library:

1. From the CommCell Console, update the media barcodes in the library. See Update the Barcode Associated with a Specific Media for step-by-step instructions.
2. Identify the Storage Policy Copies associated with the blind library. See View the Storage Policies Accessing a Library for step-by-step instructions.
3. Mark all active media associated with these Storage Policy Copies as full. This is an important step and must not be skipped.

   See Mark the Active Media of a Storage Policy Copy Full for step-by-step instructions.
4. Deconfigure the library. See Deconfigure Libraries for step-by-step instructions.
5. Configure the library as a sighted library. See Configure Devices for step-by-step instructions.

6. Right-click the primary copy associated with the library, and click **Properties**. From the **Data Paths** tab, choose the **Use preferred datapath** option.
7. Add the new data path as described in Add a Data Path to a Storage Policy Copy.

CREATE AUTOMATIC LABELING SCHEMES

Related Topic

- Automatic Labeling Schemes

Required Capability: See Capabilities and Permitted Actions

➧ To create automatic labeling schemes for stand-alone drives:

1. From the CommCell Browser, right-click the library for which you wish to create the labeling schemes and then click **Properties**.
2. Click the Media tab.
3. From the **Barcode Labeling Scheme** region, select the label and then click **Add Token**. The selected label is displayed in the box at the bottom of the region.
4. Click **OK** to save the changes.

Centera Clusters

Topics | Configure | How To | Related Topics

OVERVIEW

The Centera cluster can be configured as a disk library. The library can be configured on a MediaAgent with the Windows operating system. Centera SDK 3.2 P5 (includes support for application registration) is used by the MediaAgent software.

Before configuring the library, the Centera cluster information must be added and successfully detected, using the `Library and Drive Configuration` window. Cluster information includes the IP address or DNS name of the Centera cluster and the port ID through which the library must be accessed. See Add Centera Cluster Information and Configure Centera Cluster as a Disk Library for step-by-step instructions.

Also, appropriate Centera access requirements (for example, configuration of Centera Pea file) must be fulfilled before using the Media Agent software to backup data to Centera.

SUPPORT

Once configured, the Centera library supports all the operations supported by a disk library. Note that Centera is supported as a regular library; shared library configurations are not supported.

ADMINISTERING CENTERA DISK LIBRARIES

From the CommCell Browser, you can perform the following operations on a Centera disk library:

VIEW OR MODIFY THE PROPERTIES OF A CENTERA DISK LIBRARY

You can view the properties and modify the library name, low watermark and the status of a Centera disk library from the CommCell Console.

VIEW OR MODIFY THE PROPERTIES OF THE MOUNT PATH

You can also view the properties and modify the maximum number of readers, maximum number of writers, maximum number of readers and writers and the status of a mount path from the CommCell Console.

In addition, you can also view the configuration and space information associated with a Centera disk library. See View the Space and Access path Information for a Centera library for step-by-step instructions.

VIEW THE CONTENTS OF A MOUNT PATH

You can view the contents of a specific mount path. This feature can be used to view a list of data protection operations residing in the mount path. All the details associated with the data protection operation(s) available in the media are displayed. This includes the following:

- The Job ID and the status associated with the data protection operation
- Names of the client, agent, instance/backup set and subclient
- Whether the data protection operation is Full, Incremental, Differential or Synthetic full
- The archive file type

- The day and time in which the archive file associated with the data protection operation was created.

See View the Contents of a Mount Path for step-by-step instructions.

DELETE THE CONTENTS OF A MOUNT PATH

The delete contents option can be used to logically delete the contents of a mount path.

This operation deletes the data from the CommServe database. Note that this operation does not free-up the disk space in the mount path. A Data Aging operation must be run subsequently to free-up the disk space.

This option can be used to make media available to complete an important data protection job when there is no free-space available in the library.

> **CAUTION**
>
> Extreme caution should be exercised while using this option as once deleted, the contents of the mount path will not be available for data recovery operations.

The Delete Contents operation is recorded in the Audit Trail.

See Delete the Contents of a Mount Path for step-by-step instructions.

MIGRATE DISK LIBRARIES

You can migrate a disk library to another MediaAgent within the CommCell. Consider the following while performing this operation:

- To migrate a disk library, the target MediaAgent must have access to the same mount path as the source MediaAgent. Therefore, it is recommended that the target MediaAgent be created using mirroring. Mirroring allows one MediaAgent to be set up identically as another MediaAgent.
- If mirroring is not an option, the user must have mount paths that are accessible to the target MediaAgent. After migration, ensure that all mount paths are online or accessible.
- You can migrate a disk library if it was created in version 8.0 and the MediaAgent was upgraded to version 9.0, or if you created the disk library in version 9.0 with the EZ Operations Wizard.
- You cannot migrate a shared disk library.

See Migrate a Disk Library for step-by-step instructions.

REMOVING CENTERA CLUSTER INFORMATION

You can remove the Centera Cluster information using the `Library and Drive Configuration` window. See Remove Centera Cluster Information for step-by-step instructions

DECONFIGURING A CENTERA DISK LIBRARY

Deconfiguring a Centera disk library is similar to deconfiguring a disk library. See Deconfigure a Disk Library for step-by-step instructions.

DATA AGING ON CENTERA CLUSTERS

Consider the retention rules established in the Centera Cluster, when you set the rules for data aging on Storage Policy Copies that write data to a Centera Cluster. Retention rules should be configured based on the retention rules established in Centera as follows:

- Standard read-write access on Centera - retention rules for data aging on Storage Policy Copies will take effect.
- Worm or Compliance mode - recommended that the retention ruled for data aging on Storage policies be set to prune later than the pruning on Centera.
- Compliance Plus mode on Centera - recommended that the retention rules for data aging on Storage Policy Copies be set to "infinite".

This software supports all these modes by setting the retention property on each data object when submitting a Cclip which is used to register the data with Centera for storage. The Cclip reflects a retention date that is based on the number of retention days on the Storage Policy Copy Properties. Once the date is set on the Cclip, changing the Storage Policy Copy to a shorter retention will not change the existing Cclips and attempts to prune the data on the device will be denied until it is aged based on the Cclip value. (For information on Cclips and setting-up the data retention on Centera Clusters, refer to the Centera documentation.)

LICENSE REQUIREMENT

This feature requires a Feature License to be available in the CommServe® Server.

Review general license requirements included in License Administration. Also, View All Licenses provides step-by-step instructions on how to view the license information.

Centera Clusters - Configure

Topics | Configure | How To | Related Topics

Configure a Centera Cluster as a Disk Library

The following procedure describes the steps involved in configuring a Centera cluster as a disk library.

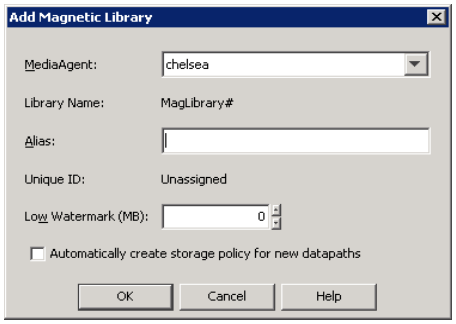
BEFORE YOU BEGIN

- Make sure that the Centera Cluster information is added. See Add Centera Cluster Information for more information.
- This feature requires a Feature License to be available in the CommServe® Server.

  Review general license requirements included in License Administration. Also, View All Licenses provides step-by-step instructions on how to view the license information.

TO CONFIGURE A CENTERA CLUSTER AS A DISK LIBRARY

1. Display the Library and Drive Configuration window.
2. From the **Library and Drive Configuration** window, click the **Start** menu, select **Centera**, and then select **Add Centera Library.**
3. In the **Add Disk Library** dialog box, select the name of the MediaAgent that will control the library and click **OK**.



Add Magnetic Library

MediaAgent: chelsea

Library Name: MagLibrary#

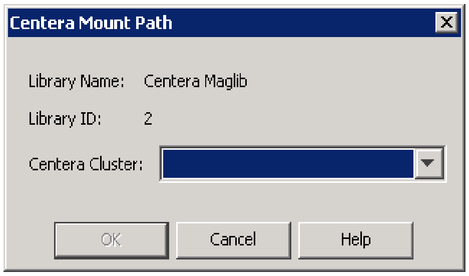
Alias:

Unique ID: Unassigned

Low Watermark (MB): 0

☐ Automatically create storage policy for new datapaths

4. In the **Centera Mount Path** dialog box, select the Centera cluster you wish to configure from the **Centera Cluster** list and click **OK**.



Centera Mount Path

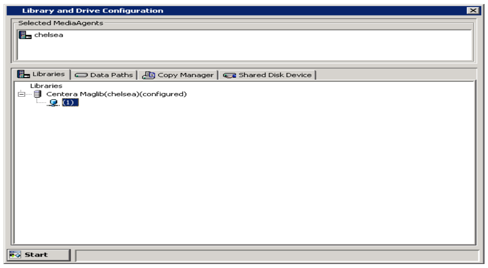
Library Name: Centera Maglib

Library ID: 2

Centera Cluster:

5. The Centera cluster is added as the mount path to the Centera disk library.

   The disk library appears in the **Library and Drive Configuration** window with the configured status.



Library and Drive Configuration

Selected MediaAgents

chelsea

Libraries

Centera Maglib(chelsea)(configured)

(1)

Centera Clusters - How To

Topics | Configure | How To | Related Topics

Add Centera Cluster Information

View the Space and Access path Information for a Centera library

View the Contents of a Mount Path

Delete the Contents of a Mount Path

Migrate a Disk Library

Remove Centera Cluster Information

Deconfigure a Disk Library

Add Centera Cluster Information

Before configuring the Centera Cluster as a disk library, the Centera Cluster information must be added using the **Library and Drive Configuration** window.

Once the Centera cluster information is added and successfully detected, the MediaAgents in the CommCell can use this information to add a Centera disk library.

The following procedure describes the steps involved in adding a Centera Cluster.

BEFORE YOU BEGIN

If you wish to use a PEA file, use the following steps to setup the environment variable for the Centera PEA file location.

1. From your computer **Desktop**, right-click **My Computer** and click **Properties**.
2. From the **Advanced** tab, click **Environment Variables**. In the **Environment Variables** dialog box, under **System Variables**, select **New**.
3. In the **Variable name** field, enter `CENTERA_PEA_LOCATION`.
4. In the **Variable value** field, add the full path to the PEA file including the file itself. For example, `C:\PEA\Centera.pea`. It is recommended that there are no spaces in either the folder location or the file name.
5. Click **OK**, and then **OK** again. Reboot the computer to commit the variable.

TO ADD THE CENTERA CLUSTER INFORMATION

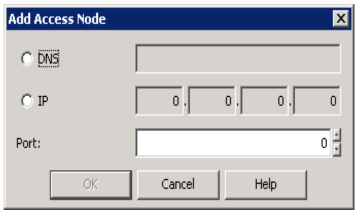
1. Display the Library and Drive Configuration window.

2. From the **Library and Drive Configuration** window, click the **Start** menu, select **Centera**, and then select **Cluster**.

3. From the **Centera Cluster List** dialog box, click on **New Cluster.**

4. From the **Centera Cluster** dialog box, click on **Add**.

5. From the **Add Access Node** dialog box, enter either the **DNS** name or **IP** address of the Centera cluster. Add a port number in the Centera cluster which can be used by the system to access it and then click **OK**.



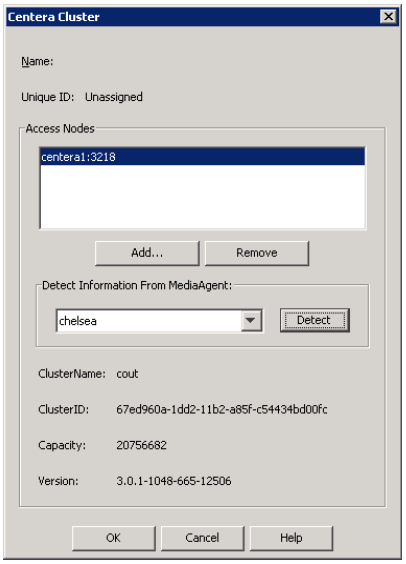
IP: 0 . 0 . 0 . 0

Port: 0

6. From the **Centera Cluster** dialog box, detect the Centera cluster using the following steps:

- Highlight the DNS name or IP address you just added from the Access Node list.
- Select the MediaAgent from which you wish to detect the Center cluster from the **Detect Information From MediaAgent** list
- Click on **Detect**.

The **ClusterName, ClusterID, Capacity** and **Version** information of the Centera cluster are displayed.



Name:

Unique ID: Unassigned

centera1:3218

Detect Information From MediaAgent: chelsea

ClusterName: cout

ClusterID: 67ed960a-1dd2-11b2-a85f-c54434bd00fc

Capacity: 20756682

Version: 3.0.1-1048-665-12506

If you encounter an error, verify and ensure that you have provided accurate information in the **Add Access Node** dialog box.

7. Click **OK**. The Centera cluster is added.

View the Space and Access Path Information for a Centera Disk Library

➨ To view the space and Access Path Information for a Centera disk library:

1. From the CommCell Console click on the Centera disk library for which you wish to view the information.

   The mount path is displayed on the right panel of the CommCell Console.

2. Right-click the mount path associated with the library and then click **Properties**.
3. Click on the Centera Info tab.

   The access path and the space information are displayed.

View the Contents of a Mount Path

Required Capability: Capabilities and Permitted Actions

➨ To view the contents of a mount path

1. From the CommCell Browser, right-click the mount path for which you wish to view the content, and then click **View Contents**.

   or

   From the Media Used By Job ID dialog box right-click the media for which you wish to view the content, and then click **View Contents**.

2. The Contents of Media dialog box displays the details of jobs available in the media.

Delete the Contents of a Mount Path

Required Capability: Capabilities and Permitted Actions

➨ To delete the contents of a mount path:

1. From the CommCell Browser, right-click the mount path for which you wish to delete the contents, and then click **Delete Contents**.
2. Click **Yes** in the Warning prompt to continue.

   Click **No** to abort the operation.

3. In the **Enter Confirmation text** dialog box, type `erase and reuse media` and then click **OK**.

   Click **Cancel** to abort the operation.

NOTES

This operation deletes the data from the CommServe database. Note that this operation does not free-up the disk space in the mount path. A Data Aging operation must be run subsequently to free-up the disk space.

Migrate a Disk Library

Required Capability: See Capabilities and Permitted Actions

Before you Begin:

Make sure that your disk library meets the appropriate criteria. For more information, see Migrate Magnetic Libraries.

➨ To perform a disk library migration from one MediaAgent to another MediaAgent:

1. Right-click the disk library that you want to migrate to another MediaAgent and click **Migrate Disk Library**.
2. A message is displayed indicating that this operation migrates the disk library to another MediaAgent. Click **OK**.
3. The Select MediaAgent dialog box is displayed. This dialog box displays the current MediaAgent that the disk library is associated with and allows you to select a MediaAgent to migrate to. From the drop-down list, select the MediaAgent you want to migrate to and click **OK**.
4. The disk library will now be associated with the selected MediaAgent. To view the disk library properties to verify successful migration, right click on the disk library where you want to view the properties, and click **Properties**.

   The MediaAgent is displayed on the **General** tab.

5. Make sure that the mount path associated with the disk library, points to valid path. (See Add or Modify Mount Paths for step-by-step instructions.)

Remove Centera Cluster Information

To remove the Centera cluster information:

1. Display the Library and Drive Configuration window.
2. From the `Library and Drive Configuration` window, click the **Start** menu, select **Centera** and then select **Cluster**.
3. From the Centera Cluster List dialog box, highlight the Centera cluster you wish to remove and then click on **Remove Cluster**.

   A **Confirm** prompt asks you to confirm the deletion of the Centera cluster.
4. Click **Yes**. The Centera cluster is removed.

Deconfigure a Disk Library

Data associated with a library will be lost, when it is deconfigured.

Before you Begin

- Be certain that the library that you want to remove is not in use. Use the Job Controller to find and kill any jobs that use the library.
- Make sure that every storage policy copy associated with the library has been deleted. Determine the storage policies accessing the library as described in View the Storage Policies Accessing a Library.

To deconfigure a disk library:

1. Display the Library and Drive Configuration window.
2. Right-click the library that you want to deconfigure, and then click **Deconfigure**.
3. A prompt appears, reminding you that the library's storage policy copies must be deleted in order for the library to be deconfigured. If no storage policy copies are associated with the library and you want to deconfigure, click **Yes**.

   The disk library is removed from the `Library and Drive Configuration` window.

Cloud Storage

Topics | Configure | How To | Tools | Support | Related Topics

OVERVIEW

Cloud Storage enables you to configure and use online storage devices — cloud storage devices — as storage targets. Cloud Storage reduces the need to maintain hardware resources such as tape or disk storage devices at onsite locations. It also provides the ability to easily increase your storage capacity as and when it is required. Cloud Storage provides centralized data access, better failover capabilities and reduces the day-to-day storage administration tasks.

As the data gets transferred over the network, protecting the integrity of data is an important aspect of any cloud storage implementation. Cloud Storage protects the integrity of the data using the following features:

- Data is transferred through secured channels using HTTPS protocol.
- Data encryption feature further encrypts the data providing data protection during network transfer as well as storage.

The deduplication feature enables you to reduce cloud storage space usage and use network bandwidth efficiently. Deduplication identifies and eliminates redundant data in the backup, reducing not only the volume of data stored in cloud but also the bandwidth required for data transfer.

See MediaAgents - Supported Features, Agents and Devices for MediaAgents that support Cloud Storage. See Cloud Storage - Support for the list of supported cloud storage vendors. Cloud Storage is supported for backup agents and migration agents.

Cloud storage libraries and devices can be identified in the CommCell Browser with icon.

The following sections explain Cloud Storage setup and implementation options.

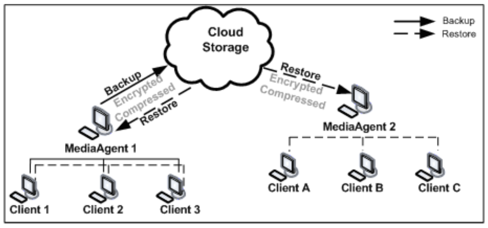
PREREQUISITES

Purchase your cloud storage account and acquire the access credentials. A list of the supported cloud storage vendors and access to their website containing account purchase information can be accessed from Cloud Storage - Support.

CLOUD AS A DIRECT STORAGE TARGET

In the direct cloud setup, the client computers are connected to the cloud library through the MediaAgent computer. During a data protection operation, the MediaAgent sends the client data directly to the cloud storage.

The diagram provides a sample direct cloud setup.



LICENSE REQUIREMENTS

Cloud Storage license is required for each MediaAgent that uses cloud storage libraries for data protection operations. This license is consumed when a cloud storage device is configured in the CommCell.

This feature requires a Feature License to be available in the CommServe® Server.

Review general license requirements included in License Administration. Also, View All Licenses provides step-by-step instructions on how to view the license information.

SET UP CLOUD STORAGE

To set up Cloud Storage:

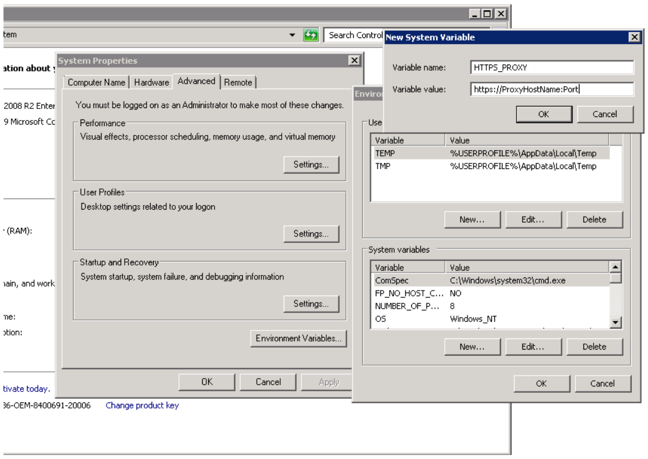
1. From the Library and Drive Configuration window, add the cloud storage hardware as a new cloud device. Provide the access credentials as required. See Add a Cloud Storage Device for step-by-step instructions.
2. Configure a new cloud storage disk library using the cloud device. See Configure a Cloud Storage Library for step-by-step instructions.

Once configured the cloud storage library operates like a regular disk library.

SETUP PROXY ON MEDIAAGENT TO CONNECT CLOUD STORAGE

If proxy server is used for internet connection on MediaAgent and if you want to use this proxy server to connect to Cloud Storage then use the following steps to set proxy information in the **Environment Variables** on the MediaAgent. This allows to send the client data to the cloud storage via proxy computer.

Use the following steps to configure cloud storage using proxy computer.



You must be logged on as an Administrator to make most of these changes.

Performance
Visual effects, processor scheduling, memory usage, and virtual memory

User Profiles
Desktop settings related to your logon

Startup and Recovery
System startup, system failure, and debugging information

New System Variable

Variable name: HTTPS_PROXY

Variable value: https://ProxyHostName:Port

OK Cancel

Variable	Value
TEMP	%USERPROFILE%\AppData\Local\Temp
TMP	%USERPROFILE%\AppData\Local\Temp

System variables

Variable	Value
ComSpec	C:\Windows\system32\cmd.exe
FP_NO_HOST_C...	NO
NUMBER_OF_P...	8
OS	Windows_NT

1. Setup proxy information in the MediaAgent computer.

   Use the following steps to setup proxy:

   - Log on to **MediaAgent** computer.
   - From the **Start Menu**, right-click the **Computer** and then click **Properties**.
   - From the **System Properties** dialog box, click **Advanced** tab.
   - Click **Environment Variables...** button.
   - In the **System Variable** area, click **New...** button.
   - In the **New System Variable** dialog box, specify the following:

     In the **Variable name** box, specify protocol to connect to Cloud Library.

     In the **Variable value** box, specify proxy server hostname and the port.
   - For HTTPS:

     ```
     HTTPS_PROXY [protocol://]<host>[:port]
     ```
   - Where:

     `<host>` - is a host name of the proxy server

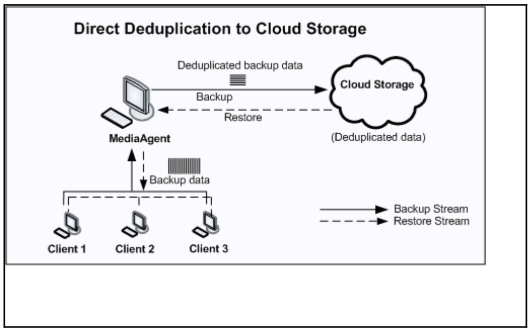
     `Port` – is a port number to communicate proxy server

   Screen shows the example of setting up HTTPS proxy.
2. Restart the MediaAgent services.
3. Add the cloud storage hardware as a new cloud device.

   See Add a Cloud Storage Device for step by step instructions.
4. Configure a new cloud storage disk library using the cloud device.

   See Configure a Cloud Storage Library for step-by-step instructions.

DIRECT DEDUPLICATION TO CLOUD STORAGE



Data backed up to a cloud storage library can be deduplicated. Deduplication eliminates redundant data segments from the backup and reduces the size of the backup data. This is particularly useful in Cloud Storage where data is transferred to the storage target over WAN. Deduplication with Cloud Storage not only reduces the storage space requirements but also reduces the data transferred over the network resulting in faster and efficient data protection operations.

Deduplication can be performed at the client or at the MediaAgent. In either case, the deduplicated data is transferred to Cloud Storage library.

The following are not supported:

- Direct Deduplication to Cloud Storage on Caringo CAStor and Dell DX Object Storage Platforms.
- Silo Storage and deduplication store reconstruction in **Direct Deduplication to Cloud Storage** configuration.

  However, Silo Storage feature is supported in Deduplication Using Cloud Gateway configuration.

LICENSE REQUIREMENTS

The following licenses are required for this configuration:

1. **Cloud Storage** license is required on all MediaAgents that operate the cloud storage library.
2. **Block Level De-Duplication** license for data deduplication. This license is required on MediaAgents hosting the Deduplication Store.

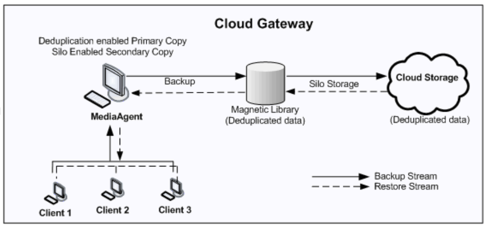
SET UP DEDUPLICATION

To deduplicate Cloud Storage backups, create Storage Policy Copies with Cloud Storage library as the storage target and enable deduplication on the copy. You can use one of following procedures.

- Deduplication - Getting Started
- Enabling Deduplication in Secondary Copies

See Deduplication to know more about the feature and its implementation.

DEDUPLICATION USING CLOUD GATEWAY



Cloud Gateway setup is a cloud storage implementation that provides the following key features:

- Local gateway to cloud storage
- Data deduplication

In the Cloud Gateway setup, a UNC path is designated as the cloud gateway. Individual clients send in their deduplicated backups to this UNC path. The deduplicated data is then moved to the Cloud Storage using Silo Storage. The cloud library is designated as the silo storage destination and data is migrated using convenient schedules.

The diagram provides a sample cloud gateway setup.

Deduplication and Silo Storage features are supported in **Deduplication Using Cloud Gateway** configuration. Please refer to the corresponding documents for more information on these features.

LICENSE REQUIREMENTS

The following licenses are required for this configuration:

1. **Cloud Storage** license is required on all MediaAgents that operate the cloud storage library.
2. **Block Level De-Duplication** for data deduplication. This license is required on MediaAgents hosting the Deduplication Store.
3. **Tape De-Duplication** license for Silo Storage. This license is required on MediaAgents hosting the Deduplication Store.

This feature requires a Feature License to be available in the CommServe® Server.

Review general license requirements included in License Administration. Also, View All Licenses provides step-by-step instructions on how to view the license information.

SET UP CLOUD GATEWAY

To set up Cloud Gateway:

1. Add the cloud storage device and configure the cloud storage library. Use the following procedures:
   - Add a Cloud Storage Device
   - Configure a Cloud Storage Library

2. Create the deduplication enabled Storage Policy Copy. See Deduplication - Getting Started for instructions.

   Auxiliary copies can also be directed to cloud libraries. See Enable Deduplication in Secondary Copy for instructions.
3. Enable Silo Storage on the Storage Policy Copy (or Copies) and select the path to Cloud Storage for the Silo data path. See Getting Started - Silo Storage for instructions.

   You will have to configure the necessary Silo Storage parameters. See Silo Storage for more discussions and recommendations.
4. Configure the client backups to use the Storage Policy Copy for data protection operations.
5. Start or Schedule the data protection operations.

CONFIGURABLE PROPERTIES

The following configuration options are available:

1. You can add a new MediaAgent to control the cloud storage library. You can add more MediaAgents for GridStor settings or restore purposes. In a Cloud Storage setup, you can add a MediaAgent from a geographically different area than the one from which the data protection is run, and restore the data to that MediaAgent. See Add a New MediaAgent to an Existing Cloud Device for instructions.
2. You can configure the mount path allocation policy defining the space allocation parameters and writer assignments. See Configure Mount Path Allocation Policy for step-by-step instructions.
3. You can configure the timeout parameter that determines how long a job waits for a status response after an operation is requested. See Modify the Mount and Unmount Timeouts for Disk Libraries for step-by-step instructions.
4. You can modify the device alias name of the cloud storage device. See View or Modify the Device Properties for Disk Libraries with Static Mount Paths for step-by-step instructions.
5. You can enable/disable the library, or enable/disable a mount path associated with the library. See Enable or Disable a Disk Library and Enable or Disable a Mount Path for step-by-step instructions.

OTHER OPERATIONS

VIEW THE CONTENTS OF A MOUNT PATH

You can view the contents of a specific mount path. This feature can be used to view a list of data protection operations residing in the mount path. All the details associated with the data protection operation(s) available in the media are displayed. This includes the following:

- The Job ID and the status associated with the data protection operation
- Names of the client, agent, instance/backup set and subclient
- Whether the data protection operation is Full, Incremental, Differential or Synthetic full
- The archive file type
- The day and time in which the archive file associated with the data protection operation was created.

See View the Contents of a Mount Path for step-by-step instructions.

VIEW THE MOUNT PATH OFFLINE REASON

The status of the disk library indicates whether the library is online or offline, and if offline, the reason for the offline status. See View the Disk Library Offline Reason for step-by-step instructions.

DELETE THE CONTENTS OF A MOUNT PATH

The delete contents option can be used to logically delete the contents of a mount path.

This operation deletes the data from the CommServe database. Note that this operation does not free-up the disk space in the mount path. A Data Aging operation must be run subsequently to free-up the disk space.

This option can be used to make media available to complete an important data protection job when there is no free-space available in the library.

> **CAUTION**
>
> Extreme caution should be exercised while using this option as once deleted, the contents of the mount path will not be available for data recovery operations.

The Delete Contents operation is recorded in the Audit Trail.

See Delete the Contents of a Mount Path for step-by-step instructions.

Considerations

Review the following considerations when using Cloud Storage:

GENERAL

A cloud storage library cannot be configured with devices that are attached to two different MediaAgents. All devices in a library must belong to the same MediaAgent.

ALTERNATE DATA PATH

Cloud storage data paths are supported as alternate data paths in GridStor settings.

However, note that data paths from deduplicated Storage Policy Copies cannot be configured as alternate data paths to cloud storage data paths, and vice versa.

DISK VOLUMES

To efficiently move data to and from the cloud storage space, the default size of disk volumes in Cloud Storage setups is set to 100 MB.

- If you wish to change this size, create the registry key DedupMagVolSzMBForSiloToCloud and set the value to desired size in MB.
- If you wish to disable this feature and follow the volume size for regular disk volumes as set in **Disk volume physical size high watermark in GB** parameter on Media Management Configuration (Service Configuration) tab, create the registry key DoNotCheckDedupMagVolSzForSiloToCloud and set the value to 1.

DATA AGING

If you have cloud storage configured with deduplication, the pruning of the data will not be done until the store is sealed and all the backup jobs associated to that store meets the retention rules for the store to become aged.

Related Reports

The Library and Drive Report can be used to review the following information.

- Name of the Cloud Storage server.
- Amount of data uploaded to the cloud library.
- Amount of data downloaded from the cloud library.

See Library and Drive Report for information on how to generate and use the report.

Frequently Asked Questions

CAN I USE DIFFERENT PORT NUMBER TO COMMUNICATE CLOUD DEVICE?

Yes. If you want to use specific port number to communicate cloud device, provide the port number with the host name.

Syntax - `[protocol://]<host>[:port]`

For example - `https://s3.amazonaws.com:1234`

Back to top

Cloud Storage - Configure

Topics | Configure | How To | Tools | Support | Related Topics

Add a Cloud Storage Device

To add a new Cloud Storage device:

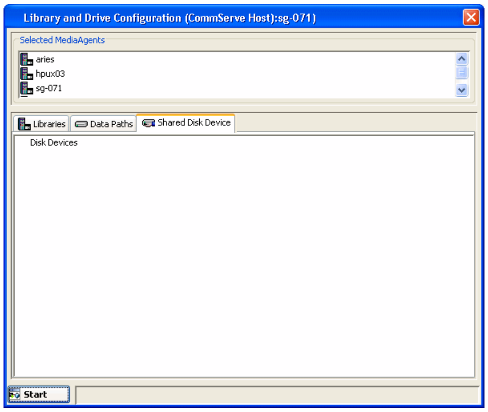
Before You Begin

- *Required Capability:* See Capabilities and Permitted Actions
- Acquire Cloud Storage access and collect the access credentials for the storage device.

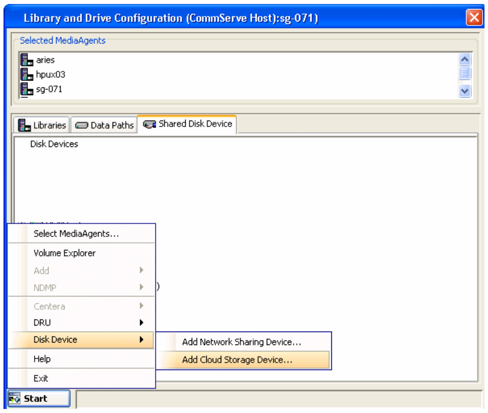
TO ADD A CLOUD STORAGE DEVICE

1. Display the Library and Drive Configuration window.

2. Click the **Shared Disk Device** tab.



3. Click the **Start** menu, select **Disk Device**, then choose **Add Cloud Storage Device.**



4. In the **Add a Cloud Storage MediaAgent** dialog box, enter or select the following information:

Device Name: System generated Cloud Storage device name.

Server Type: The type of Cloud Storage server.

MediaAgent: The name of the MediaAgent controlling the library.

Access Information

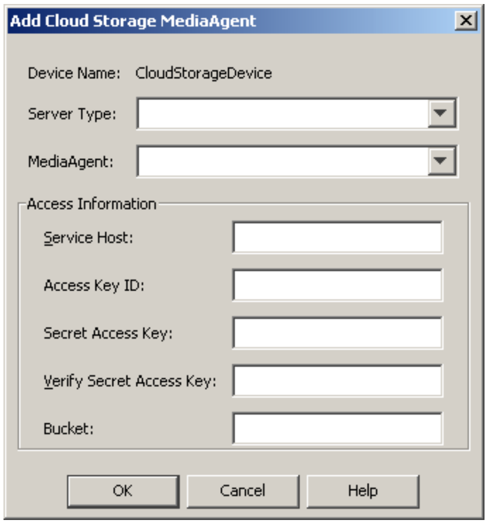
Access information consists of the credentials to access the Cloud Storage library. Acquire the access credentials from your Cloud Storage vendor and provide the necessary information.

Note that the access information for Cloud Storage devices varies for each server type, and your screen might be different from the one displayed here. See Add Cloud Storage MediaAgent for a list of server types and their access information.

- The **Access Information** details must not contain blank spaces or other special characters.
- For **Scality, Mezeo** and **Huawei UDS Massive Storage System**, select **Amazon S3** as a **Server Type** and provide the Scality information in the **Access Information** area.
- If you want to use specific port number to communicate cloud device, provide the port number with the host name.

  Syntax - [protocol://]<host>[:port]

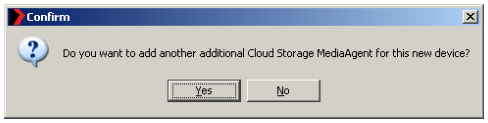
  For example - https://s3.amazonaws.com:1234


Add Cloud Storage MediaAgent

Device Name: CloudStorageDevice

5. Click **OK** to create the device.

6. If you wish to associate another MediaAgent to the device, click **Yes** in the confirmation dialog box.

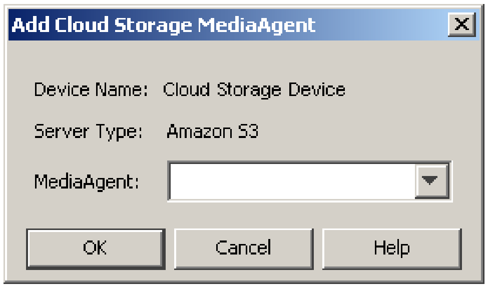


Do you want to add another additional Cloud Storage MediaAgent for this new device?

7. In the MediaAgent field, select the MediaAgent you wish to associate with the device.

   Click **OK** to save.

   If you wish to add more MediaAgents repeat steps 6 and 7 as required.



Device Name: Cloud Storage Device

Server Type: Amazon S3

MediaAgent:

CONFIGURE A CLOUD STORAGE LIBRARY

To add a new Cloud Storage library:

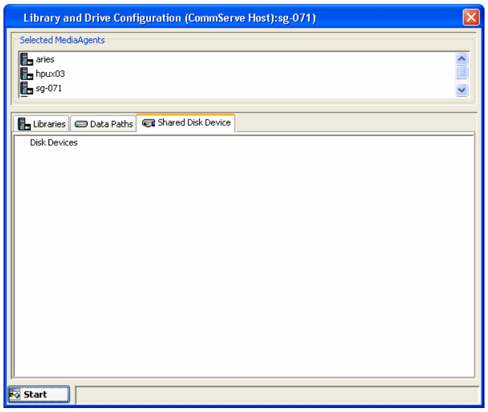
Before You Begin

Required Capability: See Capabilities and Permitted Actions

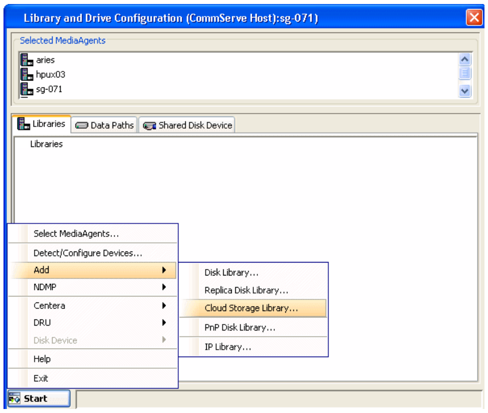
TO ADD A CLOUD STORAGE LIBRARY

1. Display the Library and Drive Configuration window.

2. Click the **Shared Disk Device** tab.



3. Click the **Start** menu, select **Add**, then choose click **Cloud Storage Disk Library.**

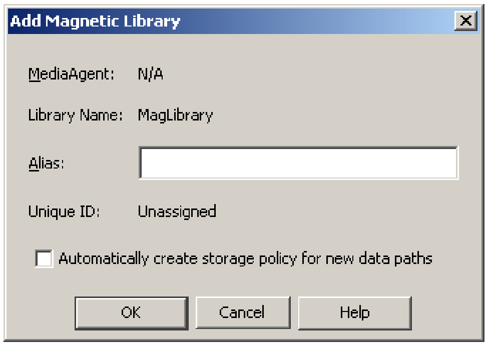


4. In the **Add Disk Library** dialog box provide the following information:

   Alias: A descriptive name for the library.

   Automatically create storage policy for new data paths: Select this option to automatically create a new storage policy when the mount path is added to this library.

   Click **OK**.



Add Magnetic Library

MediaAgent: N/A

Library Name: MagLibrary

Alias:

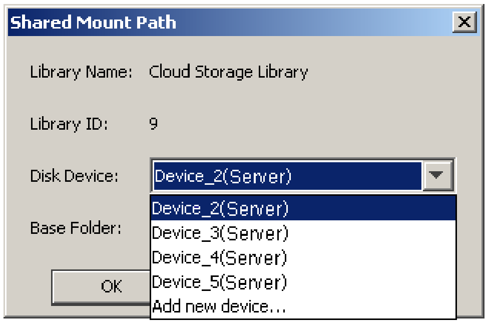
Unique ID: Unassigned

□ Automatically create storage policy for new data paths

5. In the **Shared Mount Path** dialog box provide the following information:
   - **Disk Device**: Select the name of the Cloud Storage disk device. If you wish to create a new device, select the **Add new device** option. See Add a Cloud Storage Device for instructions.
   - **Base Folder**: Provide a base folder for the library.

     Note that the base folder cannot contain blank spaces or other special characters.

   Click **OK**.



Shared Mount Path

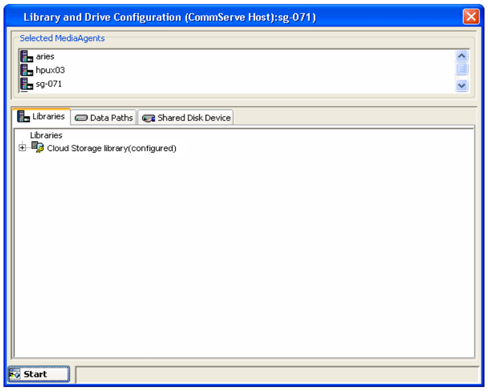
Library Name: Cloud Storage Library

Library ID: 9

Disk Device: Device_2(Server)

Base Folder:

6. The mount path is added and the Cloud Storage library appears in the **Library and Drive Configuration** window with a status of configured.



Library and Drive Configuration (CommServe Host):sg-071)

Selected MediaAgents

aries
hpux03
sg-071

Libraries

Cloud Storage library(configured)

ADD A NEW MEDIAAGENT TO AN EXISTING CLOUD DEVICE

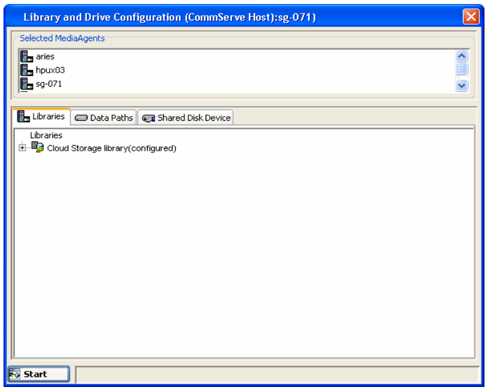
To add a new MediaAgent:

Before You Begin

- *Required Capability:* See Capabilities and Permitted Actions

TO ADD A CLOUD STORAGE DEVICE

1. Display the Library and Drive Configuration window.
2. Click the **Shared Disk Device** tab.



Library and Drive Configuration (CommServe Host):sg-071)

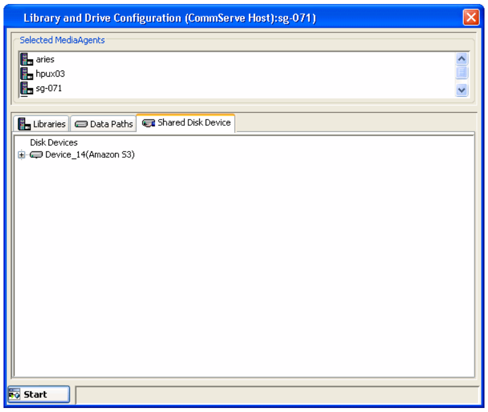
Selected MediaAgents

aries
hpux03
sg-071

Libraries

Cloud Storage library(configured)

3. Right-click the device for which you wish to add a new MediaAgent and select **Add Cloud Storage MediaAgent.**



Library and Drive Configuration (CommServe Host):sg-071)

Selected MediaAgents: aries, hpux03, sg-071

Disk Devices

Device_14(Amazon S3)

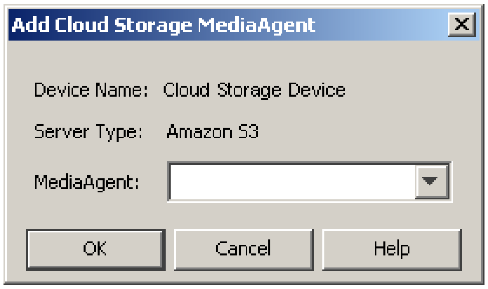
4. In the **Add a Cloud Storage MediaAgent** dialog box, select the following information:

   Device Name: System generated Cloud Storage device name.

   Server Type: The type of Cloud Storage server.

   MediaAgent: The name of the MediaAgent controlling the library.

   Click **OK** to add the MediaAgent.

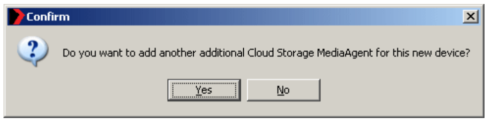


Add Cloud Storage MediaAgent

Device Name: Cloud Storage Device

Server Type: Amazon S3

5. If you wish to associate another MediaAgent to the device, click **Yes** in the confirmation dialog box.

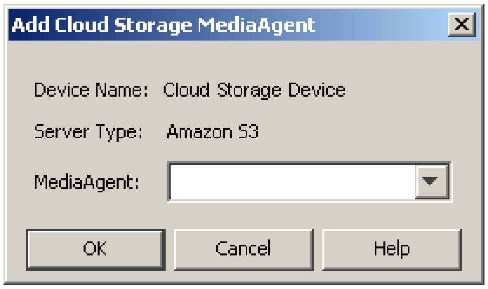


Confirm

Do you want to add another additional Cloud Storage MediaAgent for this new device?

6. In the MediaAgent field, select the MediaAgent you wish to associate with the device and click **OK** to save.

   Repeat steps 5 and 6 as required.



Add Cloud Storage MediaAgent

Device Name: Cloud Storage Device

Server Type: Amazon S3

Cloud Storage - How To

Topics | Configure | How To | Tools | Support | Related Topics

Configure Mount Path Allocation Policy

Modify the Mount and Unmount Timeouts for Disk Libraries

View or Modify the Device Properties for Disk Libraries with Static Mount Paths

Enable or Disable a Disk Library

Enable or Disable a Mount Path

View the Contents of a Mount Path

View the Disk Library Offline Reason

Delete the Contents of a Mount Path

Configure Multiple MediaAgents for a Cloud Storage Device

Deconfigure Multiple MediaAgents for a Cloud Storage Device

CONFIGURE MOUNT PATH ALLOCATION POLICY

Before You Begin

Required Capability: See Capabilities and Permitted Actions

To configure space allocation for a Cloud Storage library:

1. From the CommCell Browser, right-click the Cloud Storage mount path and then click **Properties**.
2. Click the Allocation Policy tab.
3. In the **Space Allocation** section, establish one of the following options:
   - If you prefer no space restrictions, select the **No Restriction** option.
   - To specify the maximum space that can be used by the mount path select the **Do not consume more than *n* GB** option and specify the space limit.
4. Click **OK** to save the changes.

MODIFY THE MOUNT AND UNMOUNT TIMEOUTS FOR DISK LIBRARIES

Related Topic

- Configure Timeouts

Required Capability: See Capabilities and Permitted Actions

To modify the mount and unmount timeouts for disk libraries:

1. From the CommCell Browser, right-click the disk library for which you wish to change mount and unmount timeout periods, and then click **Properties**.
2. In the **Mount** and **Unmount** box, type or select the timeout periods.
3. Click **OK** to save the changes.

VIEW OR MODIFY THE DEVICE PROPERTIES FOR DISK LIBRARIES WITH STATIC MOUNT PATHS

To modify the device properties for disk libraries with static mount paths:

1. From the CommCell Browser, right-click a mount path for which you wish to view the modify the properties, and then click **Properties**.
2. If necessary you can:
   - Change the **Device Alias Name**
   - Enable or disable the device by selecting or clearing the **Device Enabled** option.
3. Click **OK** to save the changes.

ENABLE OR DISABLE THE DISK LIBRARY

Required Capability: Capabilities and Permitted Actions

To enable or disable a disk library:

1. From the CommCell Browser, right-click the disk library that you wish to enable or disable, and then click **Properties**.
2. From the General tab of Library Properties, click the **Enable Library** option.
3. Click **OK** to save the changes.

ENABLE OR DISABLE A MOUNT PATH

Required Capability: Capabilities and Permitted Actions

To enable or disable a mount path:

1. From the CommCell Browser, right-click the mount path that you wish to enable or disable, and then click **Properties**.
2. From the General tab of Library Properties, click the **Enable MountPath** option.
3. Click **OK** to save the changes.

View the Contents of a Mount Path

Required Capability: Capabilities and Permitted Actions

To view the contents of a mount path

1. From the CommCell Browser, right-click the mount path for which you wish to view the content, and then click **View Contents**.

   or

   From the Media Used By Job ID dialog box right-click the media for which you wish to view the content, and then click **View Contents**.

2. The Contents of Media dialog box displays the details of jobs available in the media.

View the Disk Library Offline Reason

To view the offline reason for a disk library:

1. From the CommCell Browser, right-click the disk library for which you wish to view the offline reason, and then click **Properties**.

   Information on the disk library offline reason is displayed in the **Offline Reason** box.

Delete the Contents of a Mount Path

Required Capability: Capabilities and Permitted Actions

To delete the contents of a mount path:

1. From the CommCell Browser, right-click the mount path for which you wish to delete the contents, and then click **Delete Contents**.
2. Click **Yes** in the Warning prompt to continue.

   Click **No** to abort the operation.

3. In the **Enter Confirmation text** dialog box, type `erase and reuse media` and then click **OK**.

   Click **Cancel** to abort the operation.

NOTES

This operation deletes the data from the CommServe database. Note that this operation does not free-up the disk space in the mount path. A Data Aging operation must be run subsequently to free-up the disk space.

Configure Multiple MediaAgents for a Cloud Storage Device

Use the following steps to configure multiple MediaAgents for a Cloud Storage device:

1. From the CommCell Console, click the **Tools** menu and then click **Control Panel**.
2. From the **Control Panel**, double-click the **Library & Drive Configuration**.
3. From the **Select MediaAgents** dialog box, perform the following:
   - From the **Available MediaAgents** list, select the **MediaAgents** of same operating system type.
   - Click **Add >>** to move the MediaAgents to the **Selected MediaAgents** list box.
   - Click **OK**.
4. Click **OK**.
5. From the **Library and Drive Configuration** window, click the **Shared Disk Device** tab.
6. Expand the **Device** to which you want to configure multiple MediaAgents.
7. Right-click the **<Mount Path>** and then click **Configure for All Selected MediaAgents**.
   - For Windows, configure all MediaAgents when the mount path is configured as UNC path and all selected MediaAgents have access to this UNC path.
   - For Unix, ensure that the directory path to be mounted in the unconfigured MediaAgents has the same directory path as that of the configured MediaAgent.
8. Click **Yes**.

The device is configured with the list of selected **MediaAgents**.

Deconfigure Multiple MediaAgents for a Cloud Storage Device

Use the following steps to deconfigure multiple MediaAgents for a Cloud Storage Device:

1. From the CommCell Console, click the **Tools** menu and then click **Control Panel**.
2. From the **Control Panel**, double-click the **Library & Drive Configuration**.
3. From the **Select MediaAgents** dialog box, perform the following:
   - From the **Available MediaAgents** list, select the **MediaAgents** of same operating system type.
   - Click **Add >>** to move the MediaAgent(s) to the **Selected MediaAgents** list box.
   - Click **OK**.
4. Click **OK**.
5. From the **Library and Drive Configuration** window, click the **Shared Disk Device** tab.
6. Right-click the **Device** and then click **Deconfigure for All Selected MediaAgents**.
7. Click **Yes**.

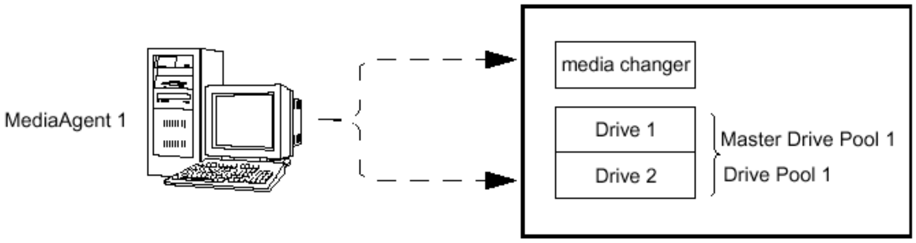
The device is deconfigured with the list of selected **MediaAgents**.

Direct-Attached Libraries

Topics | Configure | Related Topics

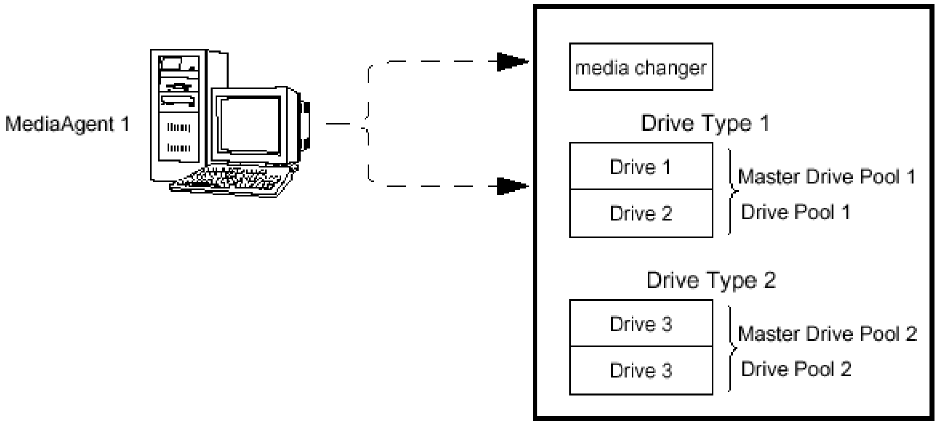
Configuring Libraries with the Same Drive Types

A direct-attached library is physically attached to the MediaAgent that controls the library. The following illustration represents a direct attached library with the same drive type..



Configuring Libraries with Mixed Drive Types

Some libraries may have different or mixed drive types. Such drives may or may not use the same type of media. The following illustration represents a direct attached library configuration, with mixed drive type.



Note that the following functions are not supported by libraries with mixed drive types:

- Exhaustive Detection
- Verify Media

Also note that libraries with mixed drive types cannot be configured on Blind Libraries.

Direct-Attached Libraries - Configure

Topics | Configure | Related Topics

CONFIGURE A DIRECT-ATTACHED LIBRARY WITH SIMILAR DRIVE TYPES

BEFORE YOU BEGIN

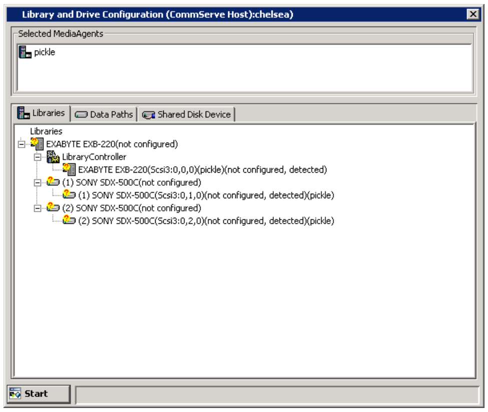
- Ensure that the hardware is configured according to the guidelines provided in Hardware Configuration Guidelines - Direct-Attached Libraries.
- Ensure that the appropriate drivers for the devices are loaded and that the operating system is able to identify the devices. For more information, see Driver Configurations.
- This feature requires a Feature License to be available in the CommServe® Server.

  Review general license requirements included in License Administration. Also, View All Licenses provides step-by-step instructions on how to view the license information.

TO CONFIGURE A DIRECT-ATTACHED LIBRARY WITH SIMILAR DRIVE TYPES

1. Display the Library and Drive Configuration window.
2. Detect the devices. Use Detection or Exhaustive Detection as required.

   Note that the **Library and Drive Configuration** window displays a master drive pool (with a drive pool and the associated drives) for the library.



```
Libraries
EXABYTE EXB-220(not configured)
    LibraryController
        EXABYTE EXB-220(Scsi3:0,0,0)(pickle)(not configured, detected)
    (1) SONY SDX-500C(not configured)
        (1) SONY SDX-500C(Scsi3:0,1,0)(not configured, detected)(pickle)
    (2) SONY SDX-500C(not configured)
        (2) SONY SDX-500C(Scsi3:0,2,0)(not configured, detected)(pickle)
```

3. Locate the library that you want to configure.

   If the library was never configured, the library status is displayed as **not configured**.

   If you want to modify library properties, right-click the library and select **Properties**.

   From the **Library Properties** window, you can change the following properties:

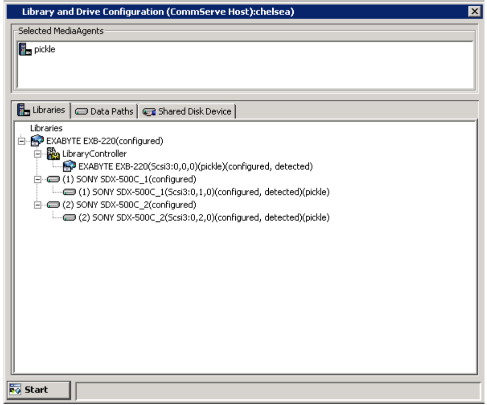
   - **Alias**: Allows you to specify a descriptive name for the library. This name is displayed in the CommCell Browser for the library. We recommend that you give each library a descriptive name for easier system administration.
   - **Door Check Seconds:** This interval, expressed in seconds, determines how frequently the system checks to see whether the library door is open. If the door is open during a check, the system conducts a full inventory of the library after the door is closed. This way, if media were manually inserted or removed from the library while the door was open, the inventory is updated. This value is editable only before the library is configured.

   When you are satisfied with your changes, click **OK**.

4. Configure the library as described in Configure Devices.

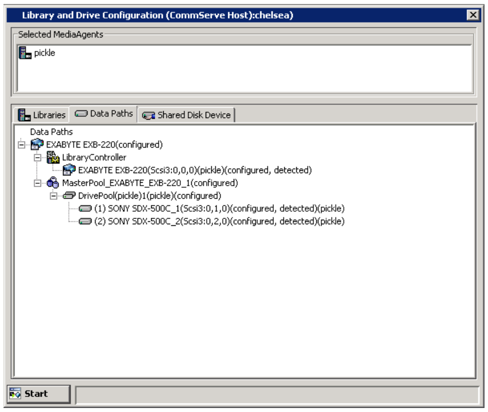
   The status of the drive pools and their constituent drives changes to `configured`.

   The **Library** tab provides the physical view of the devices (library and drives).



```
Libraries
EXABYTE EXB-220(configured)
    LibraryController
        EXABYTE EXB-220(Scsi3:0,0,0)(pickle)(configured, detected)
    (1) SONY SDX-500C_1(configured)
        (1) SONY SDX-500C_1(Scsi3:0,1,0)(configured, detected)(pickle)
    (2) SONY SDX-500C_2(configured)
        (2) SONY SDX-500C_2(Scsi3:0,2,0)(configured, detected)(pickle)
```

   The **Data Paths** tab provides a logical view of the data path used to access the devices - library, master drive pool, drive pool, drive.



```
pickle

Data Paths
EXABYTE EXB-220(configured)
    LibraryController
        EXABYTE EXB-220(Scsi3:0,0,0)(pickle)(configured, detected)
    MasterPool_EXABYTE_EXB-220_1(configured)
        DrivePool(pickle)1(pickle)(configured)
            (1) SONY SDX-500C_1(Scsi3:0,1,0)(configured, detected)(pickle)
            (2) SONY SDX-500C_2(Scsi3:0,2,0)(configured, detected)(pickle)
```

CONFIGURE A DIRECT-ATTACHED LIBRARY WITH MIXED DRIVE TYPES

BEFORE YOU BEGIN

This feature requires a Feature License to be available in the CommServe® Server.

Review general license requirements included in License Administration. Also, View All Licenses provides step-by-step instructions on how to view the license information.

TO CONFIGURE A LIBRARY WITH MIXED DRIVE TYPES

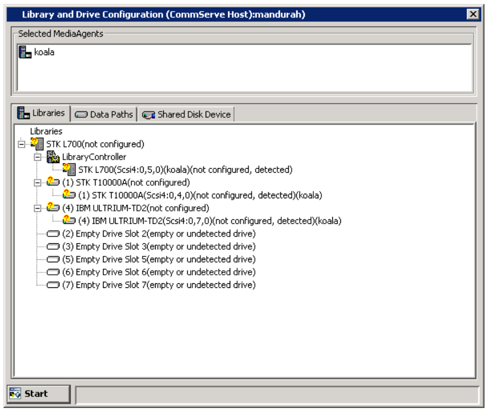
1. Display the Library and Drive Configuration window.
2. Detect the devices as described in Detect Devices.

   NOTES

   - Do not perform an exhaustive detection.

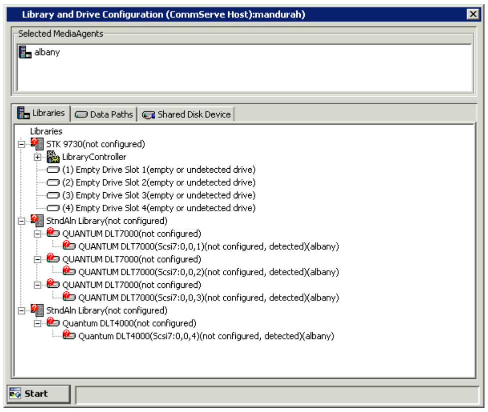
   If the library supports SCSI 3 drive identification, the system automatically detects the devices and displays them with detection status **detect success**, in the **Library and Drive Configuration** window.

   Note that the **Library and Drive Configuration** window displays a master drive pool (with a drive pool and the associated drives) for each of the drive types in the library.



```
koala

Libraries
STK L700(not configured)
    LibraryController
        STK L700(Scsi4:0,5,0)(koala)(not configured, detected)
    (1) STK T10000A(not configured)
        (1) STK T10000A(Scsi4:0,4,0)(not configured, detected)(koala)
    (4) IBM ULTRIUM-TD2(not configured)
        (4) IBM ULTRIUM-TD2(Scsi4:0,7,0)(not configured, detected)(koala)
    (2) Empty Drive Slot 2(empty or undetected drive)
    (3) Empty Drive Slot 3(empty or undetected drive)
    (5) Empty Drive Slot 5(empty or undetected drive)
    (6) Empty Drive Slot 6(empty or undetected drive)
    (7) Empty Drive Slot 7(empty or undetected drive)
```

   If the library does not support SCSI 3 drive identification, the system detects the Library with **Empty Drive Slots** and the drives as **StndAln Library**.



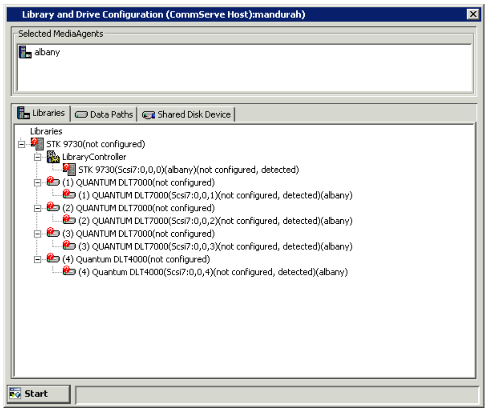
```
albany

Libraries
STK 9730(not configured)
    LibraryController
    (1) Empty Drive Slot 1(empty or undetected drive)
    (2) Empty Drive Slot 2(empty or undetected drive)
    (3) Empty Drive Slot 3(empty or undetected drive)
    (4) Empty Drive Slot 4(empty or undetected drive)
StndAln Library(not configured)
    QUANTUM DLT7000(not configured)
        QUANTUM DLT7000(Scsi7:0,0,1)(not configured, detected)(albany)
    QUANTUM DLT7000(not configured)
        QUANTUM DLT7000(Scsi7:0,0,2)(not configured, detected)(albany)
    QUANTUM DLT7000(not configured)
        QUANTUM DLT7000(Scsi7:0,0,3)(not configured, detected)(albany)
StndAln Library(not configured)
    Quantum DLT4000(not configured)
        Quantum DLT4000(Scsi7:0,0,4)(not configured, detected)(albany)
```

   Map the drives to the appropriate drive slots, by dragging the standalone drives and dropping them on the appropriate drives.

   NOTES

   Physically verify the drives and the appropriate drive slot numbers before performing this operation in the **Library and Drive Configuration** window.

The **Library** tab provides the physical view of the devices (library and drives).



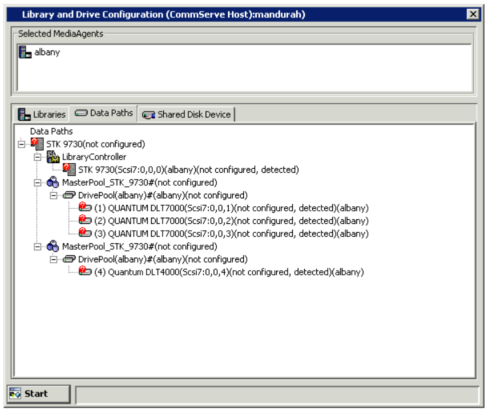
Library and Drive Configuration (CommServe Host):mandurah)

Selected MediaAgents

albany

```
Libraries
STK 9730(not configured)
    LibraryController
        STK 9730(Scsi7:0,0,0)(albany)(not configured, detected)
    (1) QUANTUM DLT7000(not configured)
        (1) QUANTUM DLT7000(Scsi7:0,0,1)(not configured, detected)(albany)
    (2) QUANTUM DLT7000(not configured)
        (2) QUANTUM DLT7000(Scsi7:0,0,2)(not configured, detected)(albany)
    (3) QUANTUM DLT7000(not configured)
        (3) QUANTUM DLT7000(Scsi7:0,0,3)(not configured, detected)(albany)
    (4) Quantum DLT4000(not configured)
        (4) Quantum DLT4000(Scsi7:0,0,4)(not configured, detected)(albany)
```

The **Data Paths** tab provides a logical view of the data path used to access the devices - library, master drive pool, drive pool, drive.



Library and Drive Configuration (CommServe Host):mandurah)

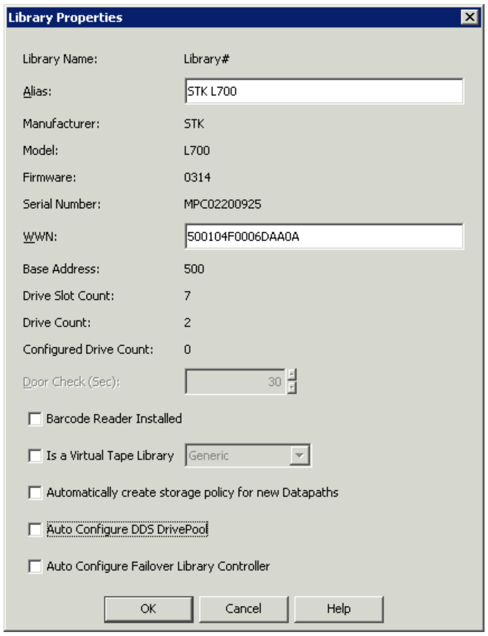
Selected MediaAgents

albany

```
Data Paths
STK 9730(not configured)
    LibraryController
        STK 9730(Scsi7:0,0,0)(albany)(not configured, detected)
    MasterPool_STK_9730#(not configured)
        DrivePool(albany)#(albany)(not configured)
            (1) QUANTUM DLT7000(Scsi7:0,0,1)(not configured, detected)(albany)
            (2) QUANTUM DLT7000(Scsi7:0,0,2)(not configured, detected)(albany)
            (3) QUANTUM DLT7000(Scsi7:0,0,3)(not configured, detected)(albany)
    MasterPool_STK_9730#(not configured)
        DrivePool(albany)#(albany)(not configured)
            (4) Quantum DLT4000(Scsi7:0,0,4)(not configured, detected)(albany)
```

3. Right-click the library and open the **Library Properties** window.

Disable the option to **Automatically create storage policy for new DataPaths**.



Library Properties

Library Name:	Library#
Alias:	STK L700
Manufacturer:	STK
Model:	L700
Firmware:	0314
Serial Number:	MPC02200925
WWN:	500104F0006DAA0A
Base Address:	500
Drive Slot Count:	7
Drive Count:	2
Configured Drive Count:	0
Door Check (Sec):	30

☐ Barcode Reader Installed

☐ Is a Virtual Tape Library Generic

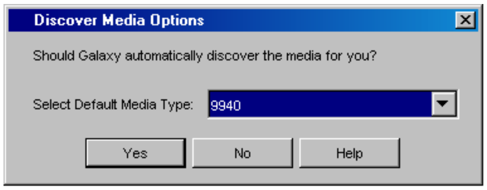
☐ Automatically create storage policy for new Datapaths

☐ Auto Configure DDS DrivePool

☐ Auto Configure Failover Library Controller

4. Configure the library as described in Configure Devices.

If this **Discover Media Options** dialog box appears during the configuration process, click **No**.



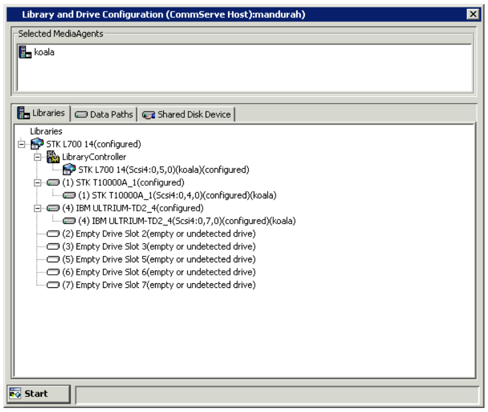
Discover Media Options

Should Galaxy automatically discover the media for you?

Select Default Media Type: 9940

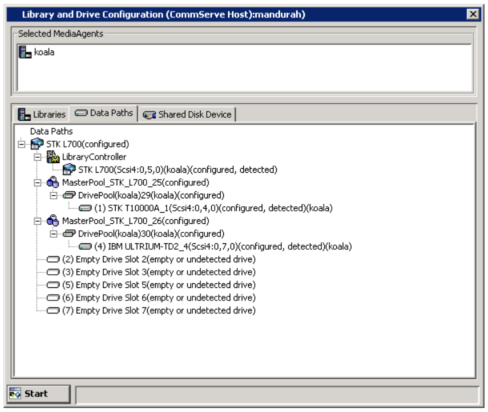
The status of the library changes to **configured** in the **Library and Drive Configuration** window.

The **Library** tab provides the physical view of the devices (library and drives).



```
koala

Libraries
STK L700 14(configured)
    LibraryController
        STK L700 14(Scsi4:0,5,0)(koala)(configured)
    (1) STK T10000A_1(configured)
        (1) STK T10000A_1(Scsi4:0,4,0)(configured)(koala)
    (4) IBM ULTRIUM-TD2_4(configured)
        (4) IBM ULTRIUM-TD2_4(Scsi4:0,7,0)(configured)(koala)
    (2) Empty Drive Slot 2(empty or undetected drive)
    (3) Empty Drive Slot 3(empty or undetected drive)
    (5) Empty Drive Slot 5(empty or undetected drive)
    (6) Empty Drive Slot 6(empty or undetected drive)
    (7) Empty Drive Slot 7(empty or undetected drive)
```

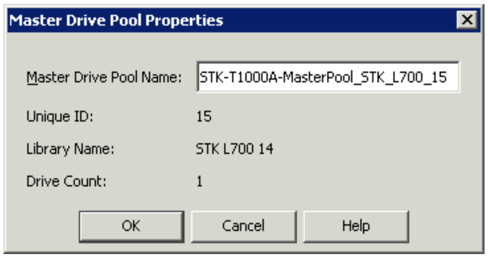
The **Data Paths** tab provides a logical view of the data path used to access the devices - library, master drive pool, drive pool, drive.



```
koala

Data Paths
STK L700(configured)
    LibraryController
        STK L700(Scsi4:0,5,0)(koala)(configured, detected)
    MasterPool_STK_L700_25(configured)
        DrivePool(koala)29(koala)(configured)
            (1) STK T10000A_1(Scsi4:0,4,0)(configured, detected)(koala)
    MasterPool_STK_L700_26(configured)
        DrivePool(koala)30(koala)(configured)
            (4) IBM ULTRIUM-TD2_4(Scsi4:0,7,0)(configured, detected)(koala)
    (2) Empty Drive Slot 2(empty or undetected drive)
    (3) Empty Drive Slot 3(empty or undetected drive)
    (5) Empty Drive Slot 5(empty or undetected drive)
    (6) Empty Drive Slot 6(empty or undetected drive)
    (7) Empty Drive Slot 7(empty or undetected drive)
```

5. Optionally, we recommend that you rename the Master Pools and Drive Pools with appropriate names, based on the drive type. This will help you to easily identify them later.

To rename a Master Pool, right-click the **MasterPool** from the **Data Path** tab and then click **Properties**. Type the new name and click **OK** to save.



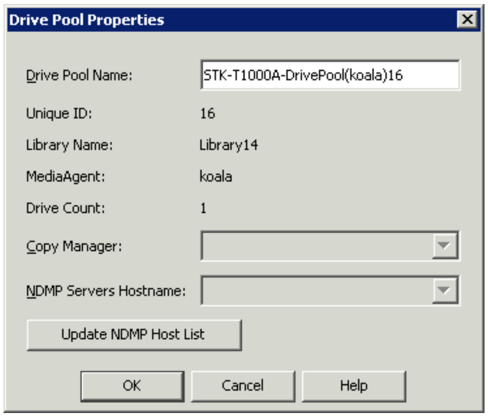
Master Drive Pool Name: STK-T1000A-MasterPool_STK_L700_15

Unique ID: 15

Library Name: STK L700 14

Drive Count: 1

To rename a Drive Pool, right-click the **DrivePool** from the **Data Path** tab and then click **Properties**. Type the new name and click **OK** to save.



Drive Pool Name: STK-T1000A-DrivePool(koala)16

Unique ID: 16

Library Name: Library14

MediaAgent: koala

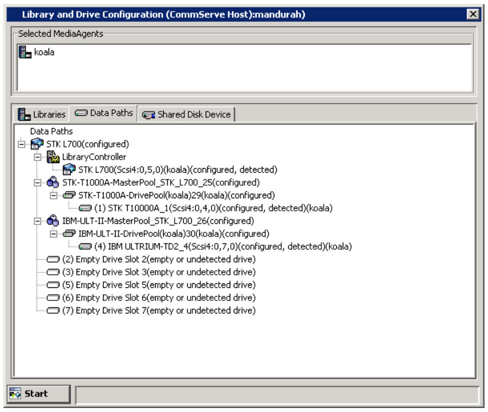
Drive Count: 1

Copy Manager:

NDMP Servers Hostname:

6. The changed names are reflected in the **Library and Drive Configuration** window.

Exit the **Library and Drive Configuration** window. To exit, click the **Start** menu and then click **Exit**.



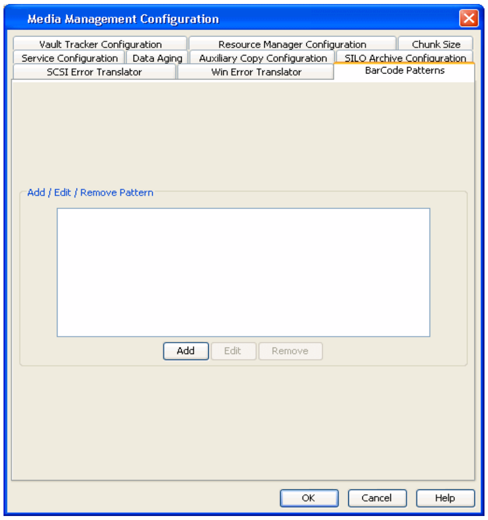
Library and Drive Configuration (CommServe Host):mandurah)

Selected MediaAgents: koala

```
Data Paths
STK L700(configured)
    LibraryController
        STK L700(Scsi4:0,5,0)(koala)(configured, detected)
    STK-T1000A-MasterPool_STK_L700_25(configured)
        STK-T1000A-DrivePool(koala)29(koala)(configured)
            (1) STK T10000A_1(Scsi4:0,4,0)(configured, detected)(koala)
    IBM-ULT-II-MasterPool_STK_L700_26(configured)
        IBM-ULT-II-DrivePool(koala)30(koala)(configured)
            (4) IBM ULTRIUM-TD2_4(Scsi4:0,7,0)(configured, detected)(koala)
    (2) Empty Drive Slot 2(empty or undetected drive)
    (3) Empty Drive Slot 3(empty or undetected drive)
    (5) Empty Drive Slot 5(empty or undetected drive)
    (6) Empty Drive Slot 6(empty or undetected drive)
    (7) Empty Drive Slot 7(empty or undetected drive)
```

7. From the CommCell Console, define the barcode patterns associated with the storage and cleaning media for each drive type.

   We highly recommend the usage of a specific barcode pattern for the media associated with each of the drive type in the library. This will help you to easily manage and administer the media in the library. (See Managing Barcodes in a Library for more information.)



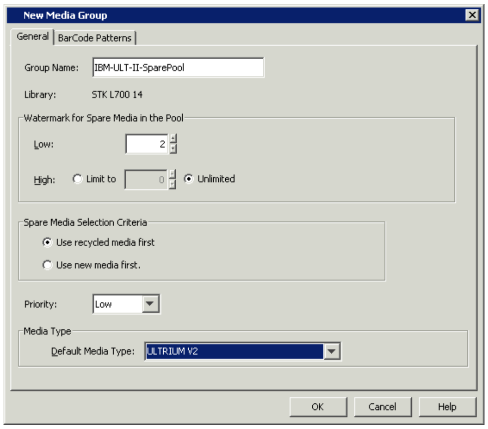
Media Management Configuration

Vault Tracker Configuration
Resource Manager Configuration
Chunk Size
Service Configuration
Data Aging
Auxiliary Copy Configuration
SILO Archive Configuration
SCSI Error Translator
Win Error Translator
BarCode Patterns
Add / Edit / Remove Pattern
Add
Edit
Remove
OK
Cancel
Help

8. Create new scratch media pools for the media associated with the various drive types.

   We recommend that you use appropriate names based on the drive type for each of the scratch media pools.

   Select the appropriate media type from the **Default Media Type** list.



New Media Group

Group Name: IBM-ULT-II-SparePool

Library: STK L700 14

Watermark for Spare Media in the Pool

Low: 2

High: ○ Limit to 0 ● Unlimited

Spare Media Selection Criteria

● Use recycled media first

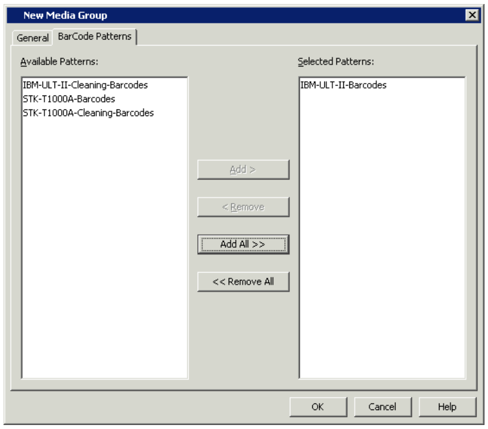
○ Use new media first.

Priority: Low

Media Type

Default Media Type: ULTRIUM V2

9. Associate the appropriate barcode pattern in each of these scratch media pools.



Available Patterns:

IBM-ULT-II-Cleaning-Barcodes
STK-T1000A-Barcodes
STK-T1000A-Cleaning-Barcodes

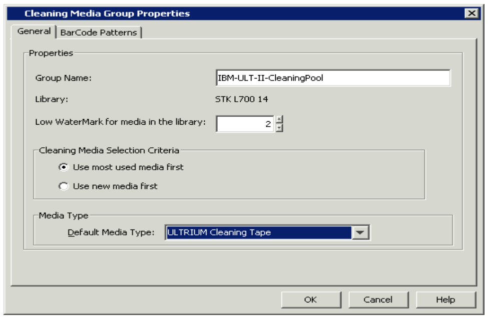
Selected Patterns:

IBM-ULT-II-Barcodes

10. Create new cleaning media pools for the cleaning media associated with the various drive types.

    We recommend that you use appropriate names based on the drive type for each of the cleaning media pools.

    Select the appropriate media type from the **Default Media Type** list.


Cleaning Media Group Properties
General
BarCode Patterns
Properties
Cleaning Media Selection Criteria
Media Type
OK
Cancel
Help

Group Name: IBM-ULT-II-CleaningPool

Library: STK L700 14

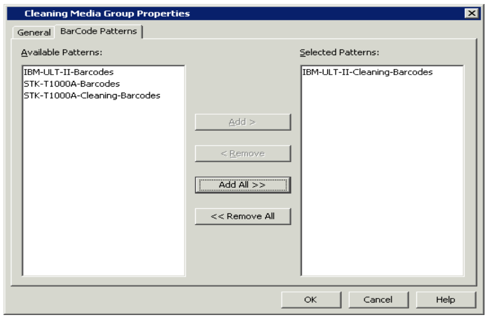
Low WaterMark for media in the library: 2

● Use most used media first

○ Use new media first

Default Media Type: ULTRIUM Cleaning Tape

11. Associate the appropriate barcode pattern in each of these cleaning media pools.



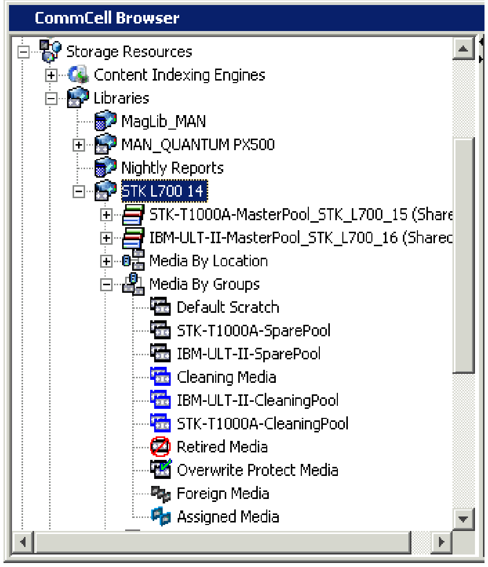
Available Patterns:

IBM-ULT-II-Barcodes
STK-T1000A-Barcodes
STK-T1000A-Cleaning-Barcodes

Selected Patterns:

IBM-ULT-II-Cleaning-Barcodes

The sample image shows the scratch and cleaning media pools with appropriate names associated with drives used in this example.



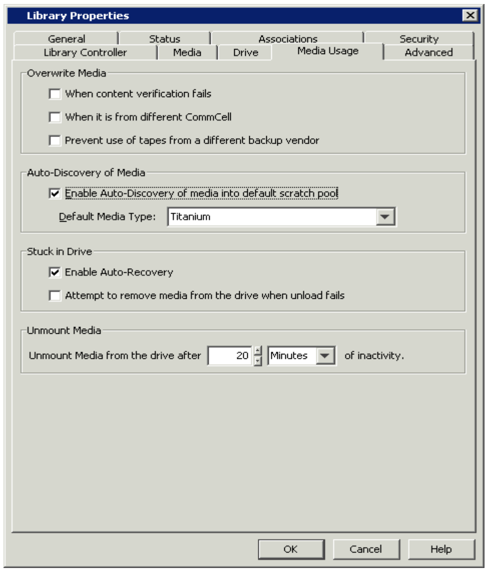
- Storage Resources
  - Content Indexing Engines
  - Libraries
    - MagLib_MAN
    - MAN_QUANTUM PX500
    - Nightly Reports
    - STK L700 14
      - STK-T1000A-MasterPool_STK_L700_15 (Share
      - IBM-ULT-II-MasterPool_STK_L700_16 (Sharec
      - Media By Location
      - Media By Groups
        - Default Scratch
        - STK-T1000A-SparePool
        - IBM-ULT-II-SparePool
        - Cleaning Media
        - IBM-ULT-II-CleaningPool
        - STK-T1000A-CleaningPool
        - Retired Media
        - Overwrite Protect Media
        - Foreign Media
        - Assigned Media

12. Open the Library Properties and enable the **Auto-Discovery of Media into default scratch pool** option.

    Select any one of the media as the **Default Media Type**.

- If media is already available in the library, they will be automatically moved into the appropriate scratch pools. If the media is not moved, perform a Full Scan or Discover Media operation.
- If media is not available in the library, the media will be automatically moved into appropriate scratch pools when you Import Media.

  If you import media that does not match the specified barcode patterns defined for the scratch pools, or is not of the media type associated with the defined scratch pools, the media will be moved to the default scratch pool. If necessary manually move them to the appropriate scratch pools.



Overwrite Media

☐ When content verification fails

☐ When it is from different CommCell

☐ Prevent use of tapes from a different backup vendor

Auto-Discovery of Media

☑ Enable Auto-Discovery of media into default scratch pool

Default Media Type: Titanium

Stuck in Drive

☑ Enable Auto-Recovery

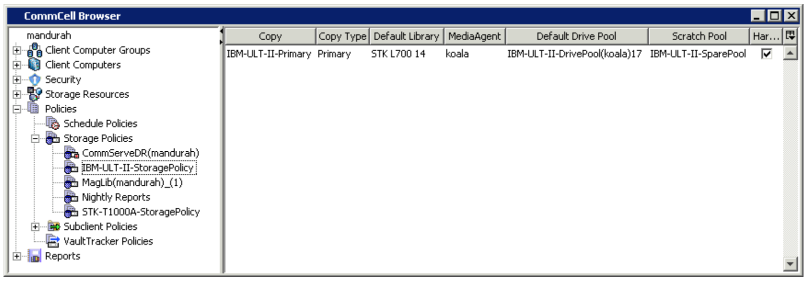
☐ Attempt to remove media from the drive when unload fails

Unmount Media

Unmount Media from the drive after 20 Minutes of inactivity.

13. Create new Storage Policies using the appropriate naming convention as recommended earlier. Associate the Storage Policy Copies to use the appropriate drive pools and scratch pools.

If you have existing storage policies, re-associate them to the appropriate drive pools and scratch pools.



Copy	Copy Type	Default Library	MediaAgent	Default Drive Pool	Scratch Pool	Har...
IBM-ULT-II-Primary	Primary	STK L700 14	koala	IBM-ULT-II-DrivePool(koala)17	IBM-ULT-II-SparePool	☑

POST CONFIGURATION CONSIDERATIONS

If you are configuring libraries with mixed drive types in a SAN do not enable the options to automatically configure the data paths in the Storage Policy Copy. (See To automatically configure the data paths in the Storage Policy Copy for more information.)

Direct-Attached Shared Libraries

Topics | Configure | Related Topics

OVERVIEW

To optimize the use of libraries and drives, the library can be configured between multiple MediaAgents in a CommCell. Although the library's media changer is attached to one MediaAgent, all MediaAgents that are attached to the library have access to the media changer through centralized software. The following are some applications of library sharing:

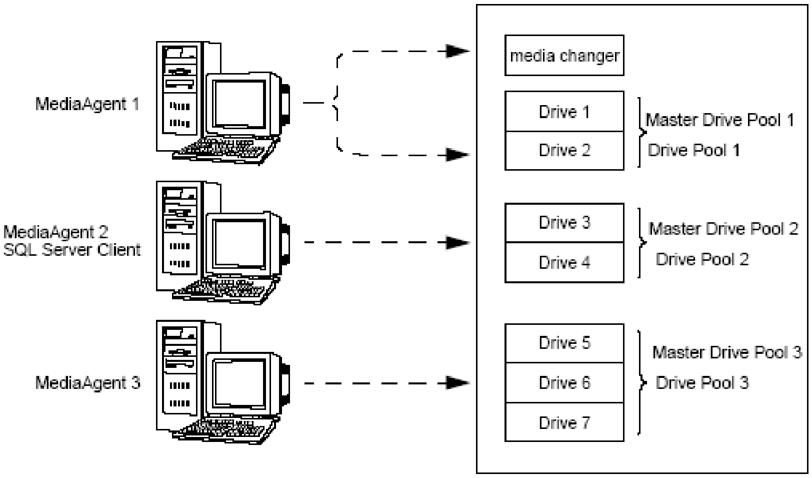
- Libraries can be shared directly with different SCSI cards, or using Storage Area Network (SAN).
- More MediaAgent processing power is available for a shared library. If you run multiple jobs simultaneously, you can improve job performance by balancing the load among MediaAgents. (For more information, refer to Load Balancing Operations Between Libraries.)
- In certain cases, you may want to eliminate network traffic by sending large amount of data secured by the data protection operation from a client computer directly to a library. For example, if you have a very large database on a client computer, you can install the MediaAgent software on the client, attach the client/MediaAgent to a library, and send the data secured by the data protection operation directly without using the network. Library sharing allows you to use some drives within a library in this fashion while keeping other drives available for normal network operations. For more information, refer to Load Balancing Operations Between Libraries.)

When configured, the shared library will include one or more master drive pools and one or more drive pools.

The Master Drive Pool contains one or more drive pools, depending on your library configuration.

Each Drive Pool contains a group of configured drives within a single library that are controlled by a specific MediaAgent The number of drives in a drive pool determines the maximum number of streams available in a Storage Policy.

The following illustration represents a direct attached shared library, in which three MediaAgents share a tape library. Note that any of these MediaAgents can also be attached to additional libraries.



In the above illustration:

- **MediaAgent 1** controls the library's media changer and Drives 1 and 2, which are assigned to Master Drive Pool 1.
- **MediaAgent 2** controls Drives 3 and 4, which are assigned to Master Drive Pool 2. This MediaAgent is also the host of a large SQL Server database with the SQL Server *i*DataAgent. To avoid loading the network with large amount of data secured by the data protection operation from this client, we have installed MediaAgent software on the computer and attached it to the library directly.
- **MediaAgent 3** controls Drive 5, Drive 6, and Drive 7, which are assigned to Master Drive Pool 3.

In order to configure a shared library properly, you must know the following about the library:

- The drive numbering within the library
- The names of the MediaAgents attached to the library
- The SCSI port and target of the drives attached to the MediaAgents

(For additional information on the relationship between drive numbering and SCSI addresses, see Understanding SCSI Mappings in the Library and Drive Configuration Window.)

If the library is configured according to the conventions detailed in Hardware Configuration Guidelines - Direct-Attached Shared Libraries, the configuration process correctly associates the SCSI target of each drive to the drive's physical position when you perform the exhaustive detection operation using the

Library and Drive Configuration window.

Direct-Attached Shared Libraries - Configure

Topics | Configure | Related Topics

Configure a Direct-Attached Shared Library

BEFORE YOU BEGIN

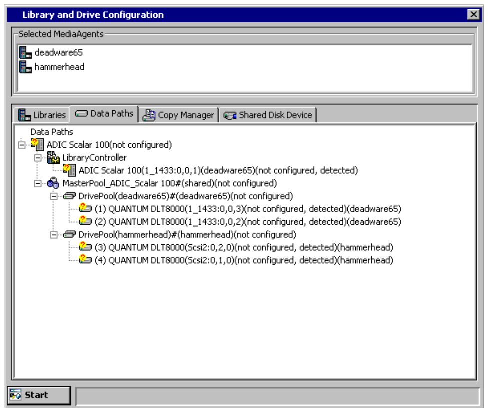
- Ensure that the hardware is configured according to the guidelines provided in Hardware Configuration Guidelines - Direct-Attached Shared Libraries.
- Ensure that the appropriate drivers for the devices are loaded and that the operating system is able to identify the devices. For more information, see Driver Configurations.
- This feature requires a Feature License to be available in the CommServe® Server.

  Review general license requirements included in License Administration. Also, View All Licenses provides step-by-step instructions on how to view the license information.

TO CONFIGURE A DIRECT-ATTACHED SHARED LIBRARY

1. Display the Library and Drive Configuration window.
2. Detect the devices. Use Detection or Exhaustive Detection as required.

   Note that the **Library and Drive Configuration** window displays a master drive pool (with a drive pool and the associated drives) for each of the MediaAgents sharing the library.



```
deadware65
hammerhead

Data Paths
ADIC Scalar 100(not configured)
  LibraryController
    ADIC Scalar 100(1_1433:0,0,1)(deadware65)(not configured, detected)
  MasterPool_ADIC_Scalar 100#(shared)(not configured)
    DrivePool(deadware65)#(deadware65)(not configured)
      (1) QUANTUM DLT8000(1_1433:0,0,3)(not configured, detected)(deadware65)
      (2) QUANTUM DLT8000(1_1433:0,0,2)(not configured, detected)(deadware65)
    DrivePool(hammerhead)#(hammerhead)(not configured)
      (3) QUANTUM DLT8000(Scsi2:0,2,0)(not configured, detected)(hammerhead)
      (4) QUANTUM DLT8000(Scsi2:0,1,0)(not configured, detected)(hammerhead)
```

3. If you want to modify library properties, right-click the library and select **Properties**.

   From the **Library Properties** window, you can change the following properties:

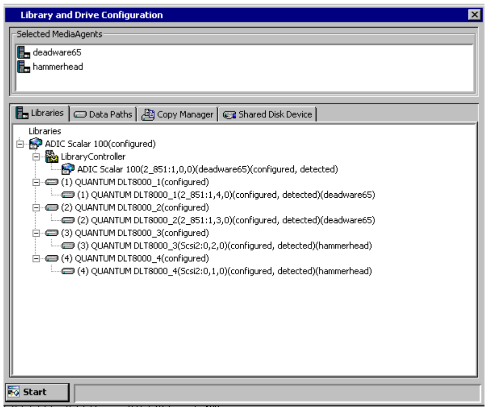
   - **Alias**: Allows you to specify a descriptive name for the library. This name is displayed in the CommCell Browser for the library. We recommend that you give each library a descriptive name for easier system administration.
   - **Door Check Seconds:** This interval, expressed in seconds, determines how frequently the system checks to see whether the library door is open. If the door is open during a check, the system conducts a full inventory of the library after the door is closed. This way, if media were manually inserted or removed from the library while the door was open, the inventory is updated. This value is editable only before the library is configured.
   - **Automatically create storage policy for new Datapaths:** This option indicates that the system must automatically create new storage policies during library configuration. This option enabled by default.

   When you are satisfied with your changes, click **OK**.

4. Configure the library as described in Configure Devices.

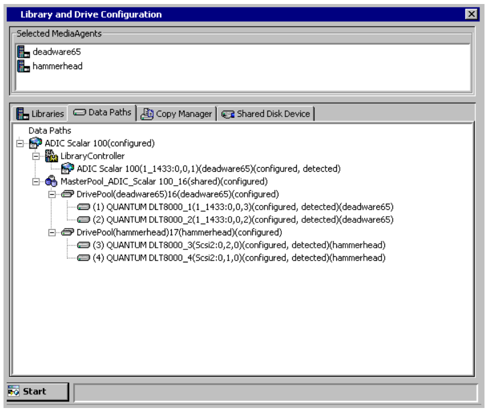
   The status of the drive pools and their constituent drives changes to `configured`.

   The **Library** tab provides the physical view of the devices (library and drives).



```
deadware65
hammerhead

Libraries
ADIC Scalar 100(configured)
  LibraryController
    ADIC Scalar 100(2_851:1,0,0)(deadware65)(configured, detected)
  (1) QUANTUM DLT8000_1(configured)
    (1) QUANTUM DLT8000_1(2_851:1,4,0)(configured, detected)(deadware65)
  (2) QUANTUM DLT8000_2(configured)
    (2) QUANTUM DLT8000_2(2_851:1,3,0)(configured, detected)(deadware65)
  (3) QUANTUM DLT8000_3(configured)
    (3) QUANTUM DLT8000_3(Scsi2:0,2,0)(configured, detected)(hammerhead)
  (4) QUANTUM DLT8000_4(configured)
    (4) QUANTUM DLT8000_4(Scsi2:0,1,0)(configured, detected)(hammerhead)
```

The **Data Paths** tab provides a logical view of the data path used to access the devices - library, master drive pool, drive pool, drive.



deadware65
hammerhead

```
Data Paths
ADIC Scalar 100(configured)
    LibraryController
        ADIC Scalar 100(1_1433:0,0,1)(deadware65)(configured, detected)
    MasterPool_ADIC_Scalar 100_16(shared)(configured)
        DrivePool(deadware65)16(deadware65)(configured)
            (1) QUANTUM DLT8000_1(1_1433:0,0,3)(configured, detected)(deadware65)
            (2) QUANTUM DLT8000_2(1_1433:0,0,2)(configured, detected)(deadware65)
        DrivePool(hammerhead)17(hammerhead)(configured)
            (3) QUANTUM DLT8000_3(Scsi2:0,2,0)(configured, detected)(hammerhead)
            (4) QUANTUM DLT8000_4(Scsi2:0,1,0)(configured, detected)(hammerhead)
```

HDS Data Retention Utility (DRU)

Topics | Configure | How To | Related Topics

OVERVIEW

HDS Data Retention Utility (DRU) in the Thunder and Lighting class of arrays can be configured as a disk library. The library can be configured on a MediaAgent with the Windows operating system.

Once configured, the HDS DRU supports all the operations supported by a disk library.

CONFIGURE A HDS DRU AS A DISK LIBRARY

The following software must be installed and the disk configured on the MediaAgent computer in which the DRU is configured:

- HDS HiCommand Device Manager Server version 4.0 must be installed, configured and set up on any one of the network machine which can see the Storage Array subsystem. Refer to HDS HiCommand Device Manager Documentation for further configuration information.
- The array be discovered and added to HDS HiCommand Device Manager Server
- CIMOM feature of HiCommand Device Manager must be activated by modifying the configuration files on HiCommand Server. See documentation of HiCommand for further configuration information.

Follow the steps described in Configure HDS DRU Disk Library for configuring the library.

ADMINISTER HDS DRU DISK LIBRARY

From the CommCell Browser, you can perform the following operations on a DRU disk library:

VIEW OR MODIFY THE PROPERTIES OF THE LIBRARY

You can view the properties and modify the library name, low watermark and the status of a disk library from the CommCell Console.

VIEW OR MODIFY THE PROPERTIES OF THE MOUNT PATH

You can also view the properties and modify the maximum number of readers, maximum number of writers, maximum number of readers and writers and the status of a mount path from the CommCell Console.

In addition, you can also view the configuration and space information associated with a disk library.

VIEW THE CONTENTS OF A MOUNT PATH

You can view the contents of a specific mount path. This feature can be used to view a list of data protection operations residing in the mount path. All the details associated with the data protection operation(s) available in the media are displayed. This includes the following:

- The Job ID and the status associated with the data protection operation

- Names of the client, agent, instance/backup set and subclient
- Whether the data protection operation is Full, Incremental, Differential or Synthetic full
- The archive file type
- The day and time in which the archive file associated with the data protection operation was created.

See View the Contents of a Mount Path for step-by-step instructions.

DELETE THE CONTENTS OF A MOUNT PATH

The delete contents option can be used to logically delete the contents of a mount path.

This operation deletes the data from the CommServe database. Note that this operation does not free-up the disk space in the mount path. A Data Aging operation must be run subsequently to free-up the disk space.

This option can be used to make media available to complete an important data protection job when there is no free-space available in the library.

> **CAUTION**
>
> Extreme caution should be exercised while using this option as once deleted, the contents of the mount path will not be available for data recovery operations.

The Delete Contents operation is recorded in the Audit Trail.

See Delete the Contents of a Mount Path for step-by-step instructions.

MIGRATE DISK LIBRARIES

You can migrate a disk library to another MediaAgent within the CommCell. Consider the following while performing this operation:

- To migrate a disk library, the target MediaAgent must have access to the same mount path as the source MediaAgent. Therefore, it is recommended that the target MediaAgent be created using mirroring. Mirroring allows one MediaAgent to be set up identically as another MediaAgent.
- If mirroring is not an option, the user must have mount paths that are accessible to the target MediaAgent. After migration, ensure that all mount paths are online or accessible.
- You cannot migrate a shared disk library.

See Migrate a Disk Library for step-by-step instructions.

DECONFIGURING A DISK LIBRARY

Deconfiguring a HDS DRU disk library is similar to deconfiguring a disk library. See Deconfigure a Disk Library for step-by-step instructions.

DATA AGING ON DRU DISK LIBRARIES

The software sets retention rules for data aging based on the values established in the Storage Policy Copies that is used to write the data in DRU disk library. Note however, if the volume is marked full (using the **Mark media full after successful operation** in the **Media** tab of the **Advanced Backup/Migration/Archive Options** dialog box) the data retention values will be set on the disk. Subsequent changes to the Storage Policy Copy, especially to a shorter retention will not change the retention time and attempts to prune the data on the device will be denied.

LICENSE REQUIREMENT

This feature requires a Feature License to be available in the CommServe® Server.

Review general license requirements included in License Administration. Also, View All Licenses provides step-by-step instructions on how to view the license information.

HDS Data Retention Utility (DRU) - Configure

Topics | Configure | How To | Related Topics

Configure HDS DRU as a Disk Library

The following procedure describes the steps involved in configuring a HDS DRU as a disk library.

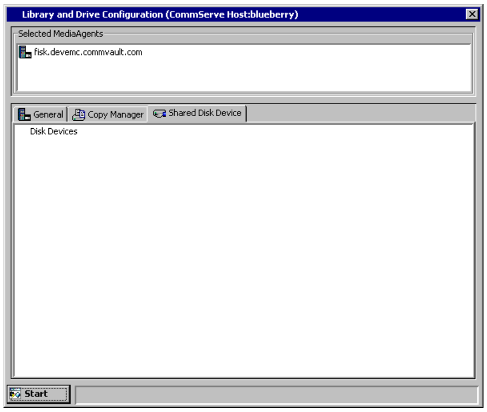
BEFORE YOU BEGIN

- The following software must be installed and the disk configured on the MediaAgent computer in which the DRU is configured:
  - HDS HiCommand Device Manager Server version 4.0 must be installed, configured and set up on any one of the network machine which can see the Storage Array subsystem. Refer to HDS HiCommand Device Manager Documentation for further configuration information.
  - The array be discovered and added to HDS HiCommand Device Manager Server
  - CIMOM feature of HiCommand Device Manager must be activated by modifying the configuration files on HiCommand Server. See documentation of HiCommand for further configuration information.
- This feature requires a Feature License to be available in the CommServe® Server.

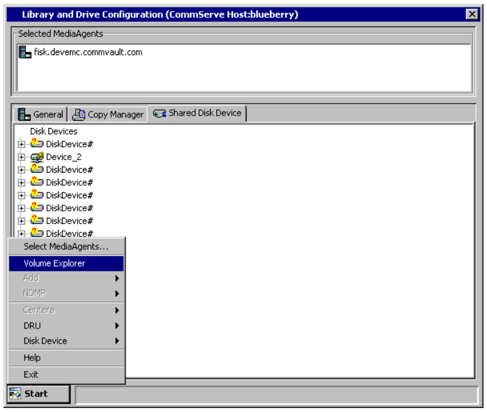
  Review general license requirements included in License Administration. Also, View All Licenses provides step-by-step instructions on how to view the license information.

TO CONFIGURE A HDS DRU AS DISK LIBRARY

1. Display the Library and Drive Configuration window.
2. Click the **Shared Disk Device** tab.

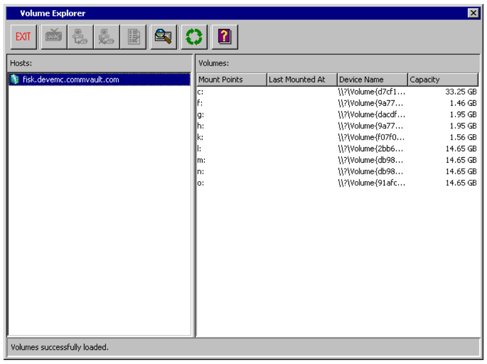

Library and Drive Configuration (CommServe Host:blueberry)
Selected MediaAgents
fisk.devemc.commvault.com
General
Copy Manager
Shared Disk Device
Disk Devices
Start

3. Click the **Start** menu, select **Volume Explorer**.



4. Click **Yes** in the **Volume Explorer** prompt warning you that the Volume Explorer is for advanced viewers.
5. From the **Hosts** pane, right-click the MediaAgent in which you wish to configure the device, and then click **Detect**.

   The disk volumes attached to the MediaAgent are displayed in the **Volumes** pane.



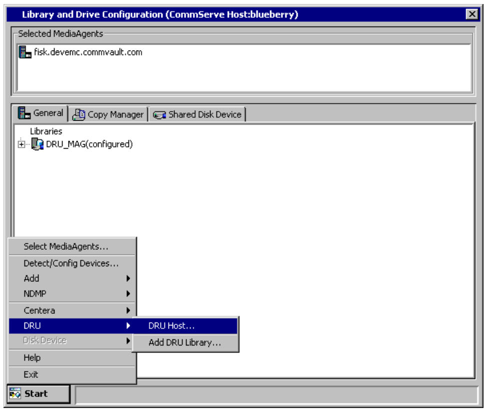
fisk.devemc.commvault.com

Mount Points	Last Mounted At	Device Name	Capacity
c:		\\?\Volume{d7cf1...	33.25 GB
f:		\\?\Volume{9a77...	1.46 GB
g:		\\?\Volume{dacdf...	1.95 GB
h:		\\?\Volume{9a77...	1.95 GB
k:		\\?\Volume{f07f0...	1.56 GB
l:		\\?\Volume{2bb6...	14.65 GB
m:		\\?\Volume{db98...	14.65 GB
n:		\\?\Volume{db98...	14.65 GB
o:		\\?\Volume{91afc...	14.65 GB

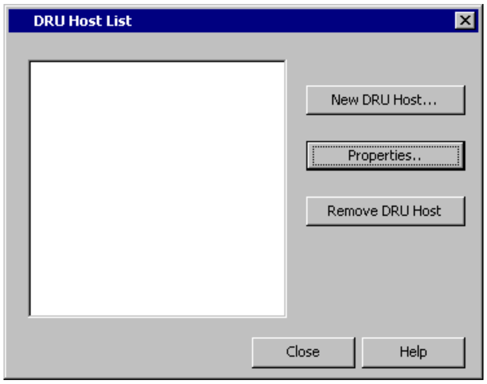
Volumes successfully loaded.

6. From the **Library and Drive Configuration** window, click the **General tab**.

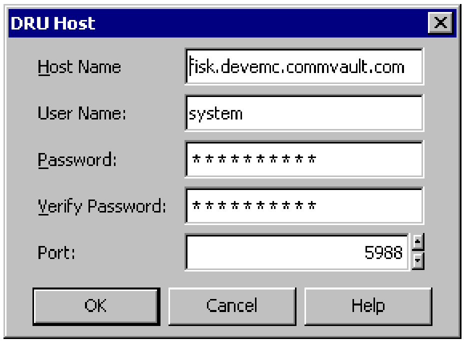
   Click the **Start** menu, select **DRU**, and then select **DRU Host**.



7. Click the **New DRU Host** button.



8. Enter the **Host name, User name, Password and Port** information and then click **OK**.



Host Name: fisk.devemc.commvault.com

User Name: system

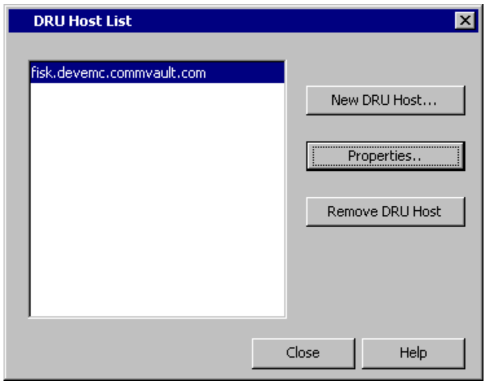
Password: **********

Verify Password: **********

Port: 5988

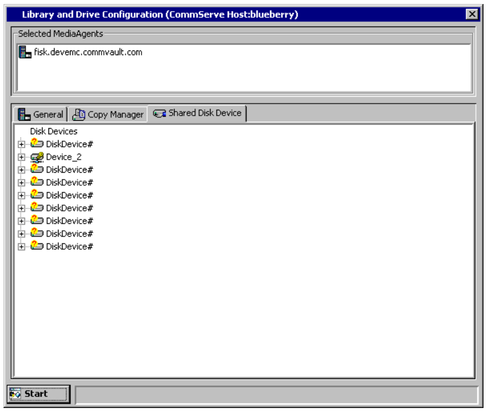
The device is displayed in the **DRU Host List**.

Click **Close**.



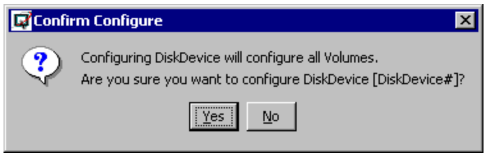
9. From the **Library and Drive Configuration** window, click the **Shared Disk Device** tab.

   All the detected volumes will be displayed.



10. Right-click the Device that you wish to configure and then click **Configure**.

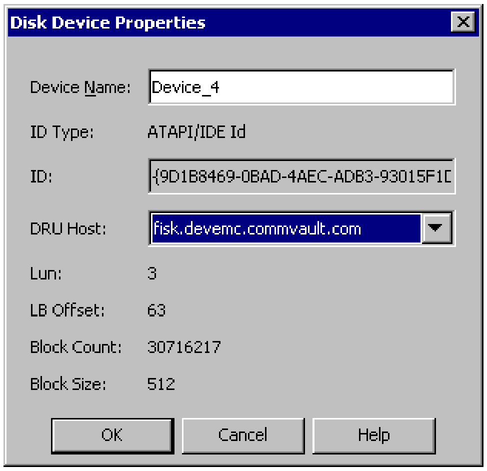
11. Click **Yes** in the **Confirm Configure** prompt.



Configuring DiskDevice will configure all Volumes.
Are you sure you want to configure DiskDevice [DiskDevice#]?

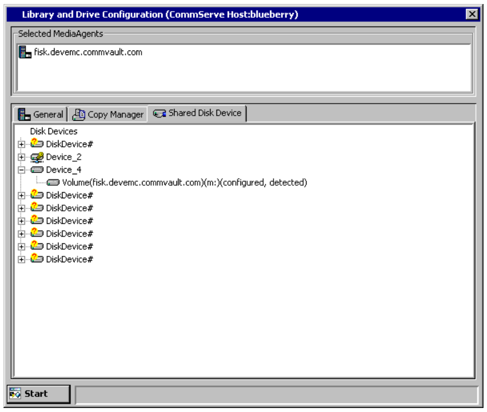
Always configure the volumes from the Disk Device. Do not individually configure the volumes.

12. Right-click the device and then click **Properties**. In the **Disk Device Properties** window, select the **DRU Host**. (This is the DRU Host that was added in step 8.)



Device Name: Device_4
ID Type: ATAPI/IDE Id
ID: {9D1B8469-0BAD-4AEC-ADB3-93015F1C
DRU Host: fisk.devemc.commvault.com
Lun: 3
LB Offset: 63
Block Count: 30716217
Block Size: 512

The DRU HOST is displayed.



13. From the **General** tab of the **Library and Drive Configuration** window, click the **Start** menu, select **DRU**, then choose **Add DRU Library.**

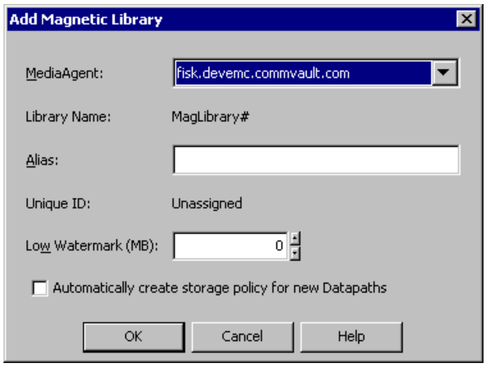
14. In the **Add Disk Library** dialog box, enter the following:

    Alias: A descriptive name for the disk library.

    Low Watermark: The minimum amount of free space at which a low watermark warning should be generated for the library.

    Automatically create storage policy for new Datapaths: Clear this option if you do not want the system to automatically create a new storage policy when a mount path is added subsequently.

    Click **OK**.


Add Magnetic Library

MediaAgent: fisk.devemc.commvault.com

Library Name: MagLibrary#

Alias:

Unique ID: Unassigned

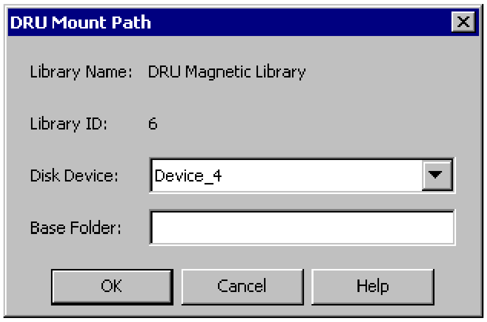
Low Watermark (MB): 0

□ Automatically create storage policy for new Datapaths

15. In the **DRU Mount Path** dialog box, select the disk device that you wish to associate as the mount path from the **Disk Device** list.

    In the **Base Folder** box, type the name of the base folder under which the mount path can store data. Do not include the drive letter while adding the name of the base folder.

    Click **OK**.


DRU Mount Path

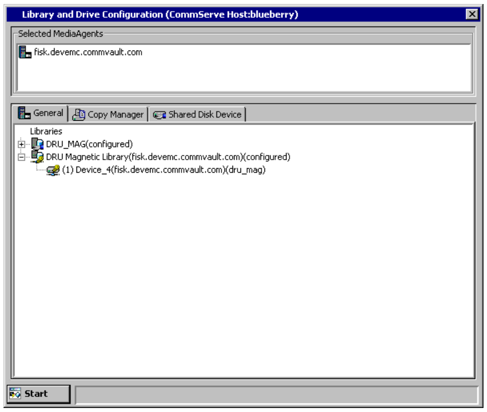
Library Name: DRU Magnetic Library

Library ID: 6

Disk Device: Device_4

Base Folder:

The disk is created as a disk library.


Library and Drive Configuration (CommServe Host:blueberry)
Selected MediaAgents
fisk.devemc.commvault.com
General
Copy Manager
Shared Disk Device
Libraries
DRU_MAG(configured)
DRU Magnetic Library(fisk.devemc.commvault.com)(configured)
(1) Device_4(fisk.devemc.commvault.com)(dru_mag)
Start

HDS Data Retention Utility (DRU) - How To

Topics | Configure | How To | Related Topics

View the Contents of a Mount Path

VIEW THE CONTENTS OF A MOUNT PATH

Required Capability: Capabilities and Permitted Actions

To view the contents of a mount path

1. From the CommCell Browser, right-click the mount path for which you wish to view the content, and then click **View Contents**.

   or

   From the Media Used By Job ID dialog box right-click the media for which you wish to view the content, and then click **View Contents**.
2. The Contents of Media dialog box displays the details of jobs available in the media.

DELETE THE CONTENTS OF A MOUNT PATH

Required Capability: Capabilities and Permitted Actions

To delete the contents of a mount path:

1. From the CommCell Browser, right-click the mount path for which you wish to delete the contents, and then click **Delete Contents**.
2. Click **Yes** in the Warning prompt to continue.

   Click **No** to abort the operation.
3. In the **Enter Confirmation text** dialog box, type `erase and reuse media` and then click **OK**.

   Click **Cancel** to abort the operation.

NOTES

This operation deletes the data from the CommServe database. Note that this operation does not free-up the disk space in the mount path. A Data Aging operation must be run subsequently to free-up the disk space.

MIGRATE A DISK LIBRARY

Required Capability: See Capabilities and Permitted Actions

To perform a disk library migration from one MediaAgent to another MediaAgent:

1. Right-click the disk library that you want to migrate to another MediaAgent and click **Migrate Disk Library**.
2. A message is displayed indicating that this operation migrates the disk library to another MediaAgent. Click **OK**.
3. The Select MediaAgent dialog box is displayed. This dialog box displays the current MediaAgent that the disk library is associated with and allows you to select a MediaAgent to migrate to. From the drop-down list, select the MediaAgent you want to migrate to and click **OK**.
4. The disk library will now be associated with the selected MediaAgent. To view the disk library properties to verify successful migration, right click on the disk library where you want to view the properties, and click **Properties**.

   The MediaAgent is displayed on the **General** tab.
5. Make sure that the mount path associated with the disk library, points to valid path. (See Add or Modify Mount Paths for step-by-step instructions.)

DECONFIGURE A DISK LIBRARY

Data associated with a library will be lost, when it is deconfigured.

Before you Begin

- Be certain that the library that you want to remove is not in use. Use the Job Controller to find and kill any jobs that use the library.
- Make sure that every storage policy copy associated with the library has been deleted. Determine the storage policies accessing the library as described in View the Storage Policies Accessing a Library.

To deconfigure a disk library:

1. Display the Library and Drive Configuration window.
2. Right-click the library that you want to deconfigure, and then click **Deconfigure**.
3. A prompt appears, reminding you that the library's storage policy copies must be deleted in order for the library to be deconfigured. If no storage policy copies are associated with the library and you want to deconfigure, click **Yes**.

   The disk library is removed from the `Library and Drive Configuration` window.

STK Libraries Attached to ACSLS Server

Topics | Configure | How To | Related Topics

OVERVIEW

StorageTek libraries controlled by an ACSLS Server can be configured. Such ACSLS controlled StorageTek libraries can be shared between:

- Multiple MediaAgents in a CommCell® group
- Multiple CommCell groups, or
- CommCell groups and others applications like Vault 98, etc.

Note that the ACSLS server computer can also be a component (either a MediaAgent or an agent) of the CommCell group. The system can share a StorageTek (STK) library with Vault98 or other applications that are accessing the STK library via ACSLS server.

SUPPORTED SOFTWARE VERSIONS

The following software versions are supported in the various components:

COMPONENT	SOFTWARE VERSION
ACSLS Server on Solaris	8.0, 8.2
STK Library Manager on Windows	2.0
MediaAgents - Windows (including Cluster)	Windows 2000 Windows 2003 Server (32 bit and 64 bit) Windows 2008 Server See System Requirements - MediaAgent for information on the platforms supported by MediaAgents.
MediaAgents - Solaris (including Cluster)	32 bit - 2.7 (Solaris 7), 2.8 (Solaris 8) 2.9 (Solaris 9) and Solaris 10 64 bit - 2.7 (Solaris 7), 2.8 (Solaris 8), 2.9 (Solaris 9) and Solaris 10 Solaris 8 32-bit and 64-bit Sun Cluster Solaris 10 x64 See System Requirements - MediaAgent for information on the platforms supported by MediaAgents.
Library Attach for Windows	1.4.3

FIREWALL CONSIDERATIONS

If the ACSLS Server and the MediaAgent computer are located on the opposite sides of firewall(s), additional ports required by the ACSLS Server, may have to be opened on the firewall(s). For more information on the necessary software and required ports, refer to STK -ACSLS documentation.

On Windows, the firewall should be configured using the Library Attach for Windows software. On Solaris install the ACSLS Client Service as described in Install ACSLS Client Service on Solaris. Follow the steps described in the Post-Install Considerations section of the above procedure to configure communication across a firewall.

CONFIGURING STK LIBRARIES ATTACHED TO ACSLS SERVER

Within a CommCell, depending on the environment, the MediaAgents can be configured to access the StorageTek library controlled by an ACSLS Server using one of the following configurations:

- Direct-attached library configuration
- Dynamic Drive Sharing (DDS) configuration in the SAN environment

In both the cases you can also have storage virtualization hardware, such as StorageTek SN6000.

The following links provide step-by-step instructions on configuring the STK library attached to an ACSLS server.

- Direct-attached Library Configuration (with or without SN6000)
- DDS Configuration (with or without SN6000)

Configuring STK Libraries with Multiple Library Storage Modules (LSM)

Libraries, such as STK SL 8500 have Library Storage Modules (LSMs). Each of these LSMs have robots on rails. Tape cartridges can be passed between each of these LSMs through pass through ports or elevators. (For detailed information on this library refer to STK documentation for the library.)

Although the entire library can be configured as a single library, to obtain optimal benefits it is recommended that each of these LSMs be configured as a logical library. This would avoid performance issues due to elevator traffic, allow for parallel robot activity and minimize the impact of a single robot failure.

The following link provides step-by-step instructions on configuring an STK library with multiple LSMs:

- Configuring STK Libraries with Multiple LSMs

Best Practices for STK Libraries Attached to ACSLS Server

- All regular library operations are supported.
- Shared ACSLS library configuration, with or without library controllers, is supported for multiple MediaAgents using different drive pools.
- During configuration, make sure to map the drive serial number to its corresponding drive ID.

  If necessary, use the following command on the ACSLS Console to display the drives and its corresponding serial number:

  ```
  display drive * -f serial_num
  ```

  This would display results similar to the following:

  ```
  2007-01-27 13:57:01 Display Drive

  Acs   Lsm   Panel    Drive Serial_num

  0     0     2        0     CX803S1909

  0     0     2        1     CX803S1939

  0     0     2        2     CX803S1959

  0     0     2        3     CX803S1979

  0     0     2        4     CX803S2259
  ```

- It is recommended that you use the exhaustive detection operation during library and drive configuration process. This will ensure that the drive serial numbers and the corresponding drive IDs are accurately mapped in the MediaAgent.
- It is recommended that the media used by the MediaAgent in the library has a specific prefix in the barcode. (e.g., SL0001, SL0002, etc.) This way you can add the entire Volume Range (SL0001-SL9999) to the scratch pool.

  If this is not possible, and if media is imported directly into the library, without using the CommCell Console, you must specify the volume range in the Library and Drive Configuration window. (See Add Volume Ranges for step-by-step instructions.)

  Whenever you import media verify and ensure that the media barcodes are within the volume range specified in the Library and Drive Configuration window. If they are outside the specified volume range, include them as described in Add Volume Ranges. If this is not done, the media available in the library will not be synchronized with the CommServe database and at some point such media may appear as exported in the CommCell Console. In such a situation, you can either add the appropriate media into the scratch pool or perform a Full Scan on the library.

- If you have multiple mail slots in the library, specify the CAP ID associated with the mail slot that will be used for importing and exporting media used by the MediaAgent. If necessary, you can also change the CAP ID if the specified CAP is busy. (See Specify the CAP ID for Importing and Exporting Media for step-by-step instructions.)
- If you notice that the library did not perform a certain operation for a long time, check the ACSSA to verify that a pending user action is completed. For example, while importing media from the CommCell Console, ensure that the media is promptly inserted and the mail slot closed.
- Avoid performing library and drive operations concurrently from both the CommCell Console and ACSSA. If you notice that a command requested by the CommCell Console did not queue successfully in ACSSA, or if you encounter problems with the subsequent operations, reset the library from the CommCell Console.
- If you have configured a library using SN6000, it is recommended that you allocate the number of drives in the Drive Allocation Policy to the number of physical drives in the library. For example, if you have 5 physical drives in the library, and you have virtualized it using SN6000 to 10 drives, set the number of drives in the Drive Allocation Policy to 5. For step-by-step instructions on how to allocate drives in a drive allocation policy, see Set the Maximum Number of Drives for each Drive Pool in a Master Drive Pool.
- Considering the following tips when you want to manage drive cleaning jobs from the CommCell Console:

  - Verify and ensure that the drive cleaning function is OFF in the STK library configuration. (not in the CommCell Console)
  - Do Not use STK cleaning barcode labels (e.g., CLNxxx) if the library does not accept them as scratch tapes. Instead they should be included in the ACSLS working pool.

    You can then Import, Discover, or Move them into Cleaning Media pool from the CommCell Console, in the same way that it is done for regular tape libraries.

- If the media is available in the library and for some reason shown as exported in the CommCell Console, use the **Set Scratch** command to move it back to the appropriate media pool. This may happen, if you performed a stuck tape recovery operation (without using the CommCell Console) or re-imported a media without using the **Import** command from the CommCell Console. (See Move a Media using the Set Scratch option for step-by-step instructions.)
- To detect the cleaning media in the library enable the **List ACSLS Clean Media** option in the **Library Properties** dialog box. (See Display Cleaning Media in the CommCell Console for step-by-step instructions.) Once enabled the cleaning cartridge available for the library's own cleaning function will be displayed in the **Media in Library** pool in the CommCell Console.

  Note that when you enable this option the library must be reset for the cleaning media to appear in the CommCell Console.

  Also this option should be enabled only in one of the configured libraries. For example, you have configured each scratch pool (from one physical library) as a CommCell library. Enable this option in any one of the configured libraries.

  To automatically detects new drives if they were swapped or replaced, enable the **Use Drive ID for Drive Replacement** in the **Library Properties** dialog box. (See Automatically Detect Replaced Drives for step-by-step instructions.) Enable this option in ACSLS Server / libraries that support a serial number for each drive ID. Type the following command in the ACSLS Console to show the serial number for all drives:

  ```
  display drive * -f serial_num
  ```

  The system will display both the drive ID and the serial number if it is supported. If it is not supported only the drive ID will be displayed.

LICENSE REQUIREMENT

This feature requires a Feature License to be available in the CommServe® Server.

Review general license requirements included in License Administration. Also, View All Licenses provides step-by-step instructions on how to view the license information.

Back to Top

STK Libraries Attached to ACSLS Server - Configure

Topics | Configure | How To | Related Topics

DIRECT-ATTACHED LIBRARY CONFIGURATION (WITH OR WITHOUT SN6000)

In a direct-attached library configuration, only Windows and Solaris MediaAgents can be configured to use the StorageTek library controlled by ACSLS server.

The following procedure describes the steps involved in configuring the STK library attached to the ACSLS Server as a direct attached library (with or without SN6000) using the `Library and Drive Configuration` window.

BEFORE YOU BEGIN

PRE-CONFIGURATION TASKS IN THE ACSLS SERVER COMPUTER

Perform the following tasks in the ACSLS Server on Solaris or STK Library Manager on Windows:

- Ensure that the hardware is configured according to the guidelines provided in Hardware Configuration Guidelines - STK Libraries Attached to ACSLS Server. (*Solaris and Windows*)
- Verify that the ACSLS server is online and the STK library is functioning. (*Solaris and Windows*)

  NOTES

  See the STK/ACSLS documentation for instructions on verifying the status of the ACSLS Server/STK library.
- In the ACSLS server, create a separate scratch pool in the library for the exclusive use of the CommCell to which the MediaAgent(s) you wish to configure are attached. (*Solaris*)

The MediaAgent uses a designated ACSLS scratch pool as its working media pool. Make sure that the designated scratch pool contains all the media that will be used by the MediaAgent. (See also: Best Practices for STK Libraries Attached to ACSLS Server)

NOTES

See the STK/ACSLS documentation for instructions on creating the scratch pool and moving the tapes to the scratch pool.

- Move the necessary tapes into this scratch pool or use the **Volume Range** in the **Library Properties** to add the necessary tapes. (Volume Range is explained in the following procedure.) (*Solaris*)

PRE-CONFIGURATION TASKS IN SN6000 (IF AVAILABLE)

Ensure the following using the SN6000 interface:

- Verify that the drives in the library are visible and configured.
- Mount Queuing is disabled.

PRE-CONFIGURATION TASKS IN THE MEDIAAGENT COMPUTER

- Ensure that the hardware is configured according to the guidelines provided in Hardware Configuration Guidelines - STK Libraries Attached to ACSLS Server.
- Install one of the following software on a Windows or Solaris MediaAgent that will act as the library controller. To configure failover library controllers, install the following software on multiple MediaAgents that will act as failover library controllers.
  - For a Windows MediaAgent, install StorageTek's *Library Attach for Windows* on the MediaAgent computer that will be configured as the Library Controller. Make sure the library is accessible through the specified ACSLS host server.

    NOTES

    See the STK/ACSLS documentation for instructions on installing the *Library Attach for Windows*.
  - For a Solaris MediaAgent, install the ACSLS Client Service. This service can be installed in one of the following ways:

    During the MediaAgent software installation on the Solaris computer. See Install the MediaAgent - Solaris for step-by-step instructions on installing the MediaAgent software on Solaris.

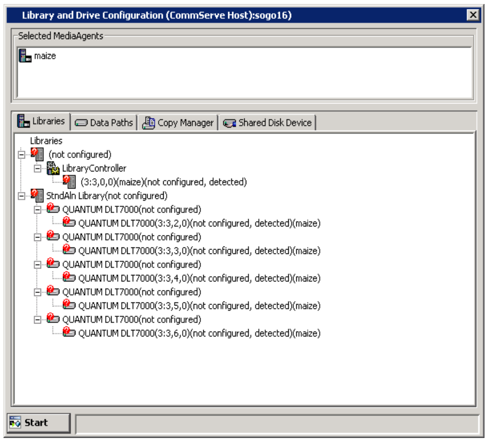
    If you have already installed the MediaAgent, you can run the `config_acsls` program on the Solaris MediaAgent computer: See Install ACSLS Client Service on Solaris for step-by-step instructions .
- This feature requires a Feature License to be available in the CommServe® Server.

  Review general license requirements included in License Administration. Also, View All Licenses provides step-by-step instructions on how to view the license information.

Required Capability: See Capabilities and Permitted Actions

CONFIGURE A STORAGETEK LIBRARY USING ACSLS SERVER AS A DIRECT-ATTACHED LIBRARY

1. Display the Library and Drive Configuration window.
2. Detect the devices that are controlled by MediaAgents that will access the library as described in Detect Devices.
3. The system detects the drives and displays them as a standalone library in the **Library and Drive Configuration** window.



```
Libraries
(not configured)
    LibraryController
        (3:3,0,0)(maize)(not configured, detected)
StndAln Library(not configured)
    QUANTUM DLT7000(not configured)
        QUANTUM DLT7000(3:3,2,0)(not configured, detected)(maize)
    QUANTUM DLT7000(not configured)
        QUANTUM DLT7000(3:3,3,0)(not configured, detected)(maize)
    QUANTUM DLT7000(not configured)
        QUANTUM DLT7000(3:3,4,0)(not configured, detected)(maize)
    QUANTUM DLT7000(not configured)
        QUANTUM DLT7000(3:3,5,0)(not configured, detected)(maize)
    QUANTUM DLT7000(not configured)
        QUANTUM DLT7000(3:3,6,0)(not configured, detected)(maize)
```

4. From the `Library and Drive Configuration` window, click the **Start** menu, choose `Add` and then select **IP Library** from the shortcut menu.
5. In the **Add Library** dialog box, enter/select the following information:

   MediaAgent: The name of the MediaAgent controlling the library.

   Library Type: The IP library type. (ACSLS)

   Library Host Name: The host name of the ACSLS server. If you have SN6000 attached, the host name of SN6000.

   Work Pool Number:

If the library is controlled by the ACSLS Server on Solaris, enter the work pool number associated with the work pool created for the system in the ACSLS server.

If the library is controlled by the STK Library Manager on Windows, the work pool number should be 0.

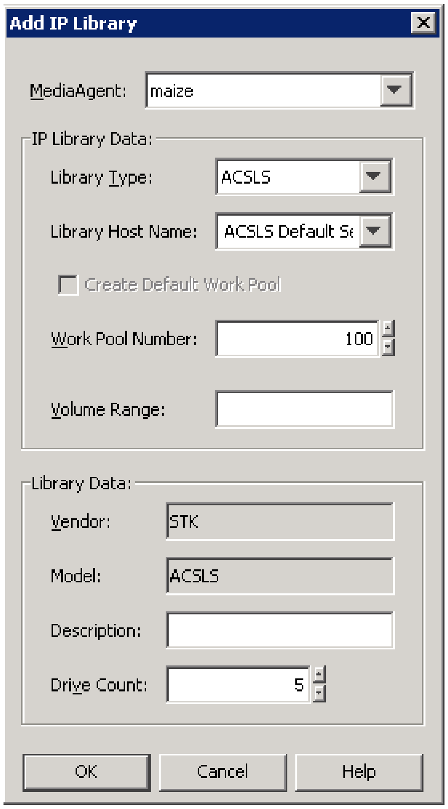
Volume Range: The ascending barcode range(s) of volumes available in the specified work pool. Use a dash to specify range and commas to delimit ranges. For example: 000065-000165,000167,000170-000199.

Vendor: The manufacturer of the library. (STK)

Model: The library model. (ACSLS)

Description: An optional field into which you can enter a description for the library

Drive Count: The number of drives in the library.



Add IP Library

MediaAgent: maize

IP Library Data:

Library Type: ACSLS

Library Host Name: ACSLS Default Se

□ Create Default Work Pool

Work Pool Number: 100

Volume Range:

Library Data:

Vendor: STK

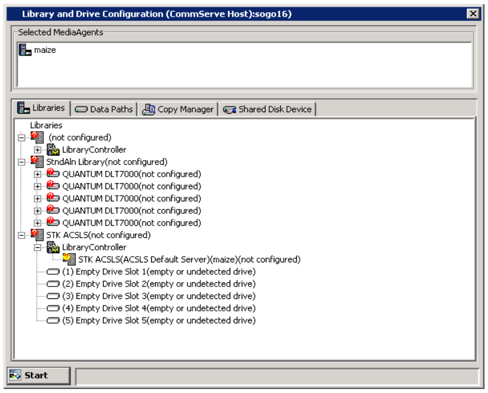
Model: ACSLS

Description:

Drive Count: 5

6. When you are finished, click **OK**.

The system detects the library and displays the library information in the **Library and Drive Configuration** window.



Library and Drive Configuration (CommServe Host):sogo16)

Selected MediaAgents

maize

```
Libraries
(not configured)
    LibraryController
StndAln Library(not configured)
    QUANTUM DLT7000(not configured)
    QUANTUM DLT7000(not configured)
    QUANTUM DLT7000(not configured)
    QUANTUM DLT7000(not configured)
    QUANTUM DLT7000(not configured)
STK ACSLS(not configured)
    LibraryController
        STK ACSLS(ACSLS Default Server)(maize)(not configured)
    (1) Empty Drive Slot 1(empty or undetected drive)
    (2) Empty Drive Slot 2(empty or undetected drive)
    (3) Empty Drive Slot 3(empty or undetected drive)
    (4) Empty Drive Slot 4(empty or undetected drive)
    (5) Empty Drive Slot 5(empty or undetected drive)
```

7. If you want to modify the library properties, right-click the library and select **Properties**.

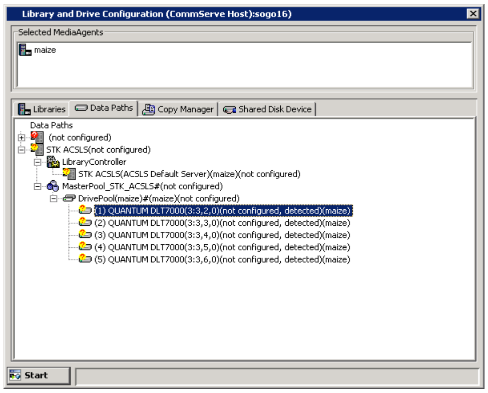
From the **Library Properties** dialog box, you can change the following properties:

Alias: The user-defined name for the library. This name is displayed in the CommCell Console for the library. We recommend that you give each library a descriptive name as its Alias, for easier system administration.

When you are satisfied with your changes, click **OK**.

8. Highlight the **MasterPool** from the `StandAln` library and then drag and drop it on the `STK ACSLS` library.

The devices are displayed in the library tree with detection status `not configured`, `detect success` in the **Library and Drive Configuration** window.



Library and Drive Configuration (CommServe Host):sogo16)

Selected MediaAgents: maize

```
Data Paths
(not configured)
STK ACSLS(not configured)
    LibraryController
        STK ACSLS(ACSLS Default Server)(maize)(not configured)
    MasterPool_STK_ACSLS#(not configured)
        DrivePool(maize)#(maize)(not configured)
            (1) QUANTUM DLT7000(3:3,2,0)(not configured, detected)(maize)
            (2) QUANTUM DLT7000(3:3,3,0)(not configured, detected)(maize)
            (3) QUANTUM DLT7000(3:3,4,0)(not configured, detected)(maize)
            (4) QUANTUM DLT7000(3:3,5,0)(not configured, detected)(maize)
            (5) QUANTUM DLT7000(3:3,6,0)(not configured, detected)(maize)
```

9. If you are not sure of the drive serial number and ACSLS drive ID mapping, then perform an exhaustive detection of the devices from the Library Controller level.

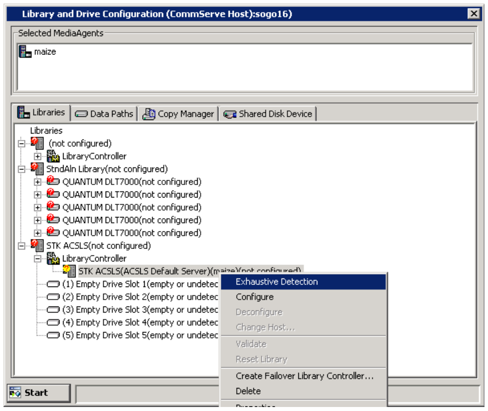
This will ensure that the drives are mapped to the appropriate serial number.

If necessary, use the following command on the ACSLS Console to display the drives and its corresponding serial number:

```
display drive * -f serial_num
```

This would display results similar to the following:

```
2007-01-27 13:57:01 Display Drive

Acs   Lsm   Panel   Drive  Serial_num

0     0     2       0      CX803S1909

0     0     2       1      CX803S1939

0     0     2       2      CX803S1959

0     0     2       3      CX803S1979

0     0     2       4      CX803S2259
```



Library and Drive Configuration (CommServe Host):sogo16)

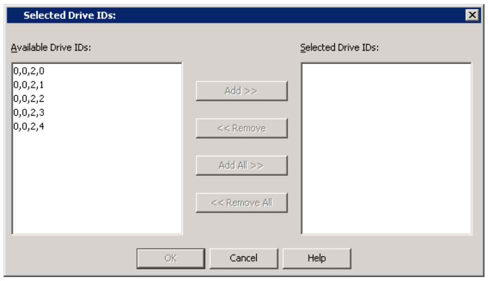
Selected MediaAgents: maize

```
Libraries
(not configured)
    LibraryController
StndAln Library(not configured)
    QUANTUM DLT7000(not configured)
    QUANTUM DLT7000(not configured)
    QUANTUM DLT7000(not configured)
    QUANTUM DLT7000(not configured)
    QUANTUM DLT7000(not configured)
STK ACSLS(not configured)
    LibraryController
        STK ACSLS(ACSLS Default Server)(maize)(not configured)
    (1) Empty Drive Slot 1(empty or undetec
    (2) Empty Drive Slot 2(empty or undetec
    (3) Empty Drive Slot 3(empty or undetec
    (4) Empty Drive Slot 4(empty or undetec
    (5) Empty Drive Slot 5(empty or undetec
```

Select the most likely drives or all the available drives in the `Select Drive IDs` dialog box.

NOTES

As this process attempts to mount a media in each of the selected drives to determine the drive numbers to its correct serial number, depending on the number of drives selected, this operation may take some time to complete.



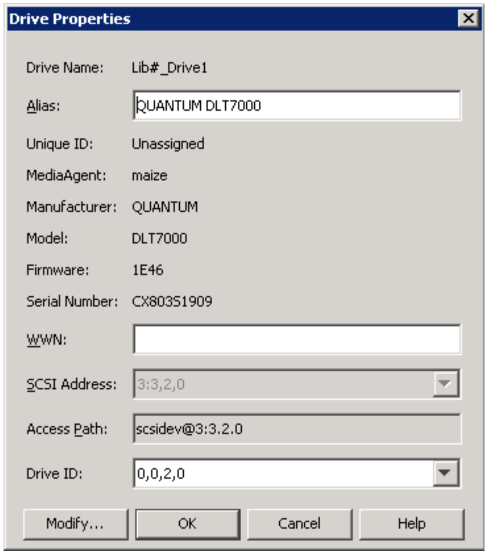
Selected Drive IDs:

Available Drive IDs:

0,0,2,0
0,0,2,1
0,0,2,2
0,0,2,3
0,0,2,4

Selected Drive IDs:

Right-click the drive and then click **Properties**. In the **Drive Properties** dialog box, verify that the Drive **Serial Number** matches the **Drive ID**.



Drive Properties

Drive Name: Lib#_Drive1

Alias: QUANTUM DLT7000

Unique ID: Unassigned

MediaAgent: maize

Manufacturer: QUANTUM

Model: DLT7000

Firmware: 1E46

Serial Number: CX803S1909

WWN:

SCSI Address: 3:3,2,0

Access Path: scsidev@3:3.2.0

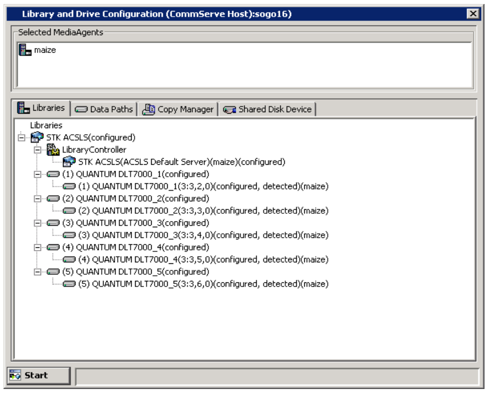
Drive ID: 0,0,2,0

10. Configure the library as described in Configure Devices.

The devices are displayed as `configured, detect success`.

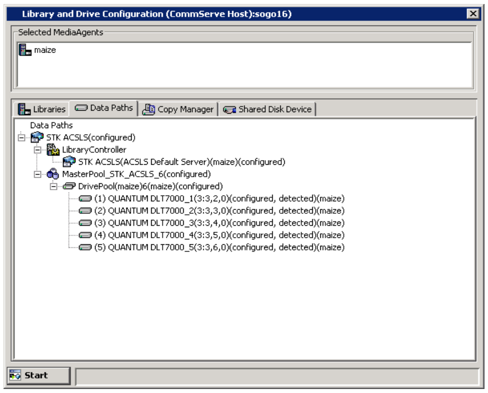
The **Library** tab provides the physical view of the devices (library and drives).

NOTES:You can validate the physical drive configuration by selecting **Validate,** from the drive, drive pool or library level.



```
maize

Libraries
⊟ STK ACSLS(configured)
    ⊟ LibraryController
        STK ACSLS(ACSLS Default Server)(maize)(configured)
    ⊟ (1) QUANTUM DLT7000_1(configured)
        (1) QUANTUM DLT7000_1(3:3,2,0)(configured, detected)(maize)
    ⊟ (2) QUANTUM DLT7000_2(configured)
        (2) QUANTUM DLT7000_2(3:3,3,0)(configured, detected)(maize)
    ⊟ (3) QUANTUM DLT7000_3(configured)
        (3) QUANTUM DLT7000_3(3:3,4,0)(configured, detected)(maize)
    ⊟ (4) QUANTUM DLT7000_4(configured)
        (4) QUANTUM DLT7000_4(3:3,5,0)(configured, detected)(maize)
    ⊟ (5) QUANTUM DLT7000_5(configured)
        (5) QUANTUM DLT7000_5(3:3,6,0)(configured, detected)(maize)
```

The **Data Paths** tab provides a logical view of the data path used to access the devices - library, master drive pool, drive pool, drive.



```
maize

Data Paths
⊟ STK ACSLS(configured)
    ⊟ LibraryController
        STK ACSLS(ACSLS Default Server)(maize)(configured)
    ⊟ MasterPool_STK_ACSLS_6(configured)
        ⊟ DrivePool(maize)6(maize)(configured)
            (1) QUANTUM DLT7000_1(3:3,2,0)(configured, detected)(maize)
            (2) QUANTUM DLT7000_2(3:3,3,0)(configured, detected)(maize)
            (3) QUANTUM DLT7000_3(3:3,4,0)(configured, detected)(maize)
            (4) QUANTUM DLT7000_4(3:3,5,0)(configured, detected)(maize)
            (5) QUANTUM DLT7000_5(3:3,6,0)(configured, detected)(maize)
```

POST CONFIGURATION CONSIDERATIONS

- If you have multiple mail slots in the library, you must specify the CAP ID associated with the mail slot that will be used for importing and exporting media. (See Specify the CAP ID for Importing and Exporting Media for step-by-step instructions.)
- If you have configured a library using SN6000, it is recommended that you allocate the number of drives in the Drive Allocation Policy to the number of physical drives in the library. For example, if you have 5 physical drives in the library, and you have virtualized it using SN6000 to 10 drives, set the number of drives in the Drive Allocation Policy to 5. For step-by-step instructions on how to allocate drives in a drive allocation policy, see Set the Maximum Number of Drives for each Drive Pool in a Master Drive Pool.

DDS CONFIGURATION (WITH OR WITHOUT SN6000)

In a DDS configuration, all MediaAgents can be configured provided you have at least one Windows or Solaris MediaAgent. (This MediaAgent is referred to as the primary MediaAgent in this section.)

The following procedure describes the steps involved in configuring the STK library attached to the ACSLS Server as a direct attached library (with or without SN6000) using the **Library and Drive Configuration** window.

BEFORE YOU BEGIN

PRE-CONFIGURATION TASKS IN THE ACSLS SERVER COMPUTER

Perform the following tasks in the ACSLS Server on Solaris or STK Library Manager on Windows:

- Ensure that the hardware is configured according to the guidelines provided in Hardware Configuration Guidelines - STK Libraries Attached to ACSLS Server. (*Solaris and Windows*)
- Verify that the ACSLS server is online and the STK library is functioning. (*Solaris and Windows*)

  NOTES

  See the STK/ACSLS documentation for instructions on verifying the status of the ACSLS Server/STK library.
- In the ACSLS server, create a separate scratch pool in the library for the exclusive use of the CommCell to which the MediaAgent(s) you wish to configure are attached. (*Solaris*)

  The MediaAgent uses a designated ACSLS scratch pool as its working media pool. Make sure that the designated scratch pool contains all the media that will be used by the MediaAgent. (See also: Best Practices for STK Libraries Attached to ACSLS Server)

  NOTES

  See the STK/ACSLS documentation for instructions on creating the scratch pool and moving the tapes to the scratch pool.
- Move the necessary tapes into this scratch pool or use the **Volume Range** in the **Library Properties** to add the necessary tapes. (Volume Range is

explained in the following procedure.) (*Solaris*)

PRE-CONFIGURATION TASKS IN SN6000 (IF AVAILABLE)

Ensure the following using the SN6000 interface:

- Verify that the drives in the library are visible and configured.
- Mount Queuing is disabled.

PRE-CONFIGURATION TASKS IN THE MEDIAAGENT COMPUTER

- Ensure that the hardware is configured according to the guidelines provided in Hardware Configuration Guidelines - STK Libraries Attached to ACSLS Server.
- Install one of the following software on a Windows or Solaris MediaAgent that will act as the library controller. To configure failover library controllers, install the following software on multiple MediaAgents that will act as failover library controllers.
  - For a Windows MediaAgent, install StorageTek's *Library Attach for Windows* on the MediaAgent computer that will be configured as the Library Controller. Make sure the library is accessible through the specified ACSLS host server.

    NOTES

    See the STK/ACSLS documentation for instructions on installing the *Library Attach for Windows*.
  - For a Solaris MediaAgent, install the ACSLS Client Service. This service can be installed in one of the following ways:

    During the MediaAgent software installation on the Solaris computer. See Install the MediaAgent - Solaris for step-by-step instructions on installing the MediaAgent software on Solaris.

    If you have already installed the MediaAgent, you can run the `config_acsls` program on the Solaris MediaAgent computer: See Install ACSLS Client Service on Solaris for step-by-step instructions .
- This feature requires a Feature License to be available in the CommServe® Server.

  Review general license requirements included in License Administration. Also, View All Licenses provides step-by-step instructions on how to view the license information.

Required Capability: See Capabilities and Permitted Actions

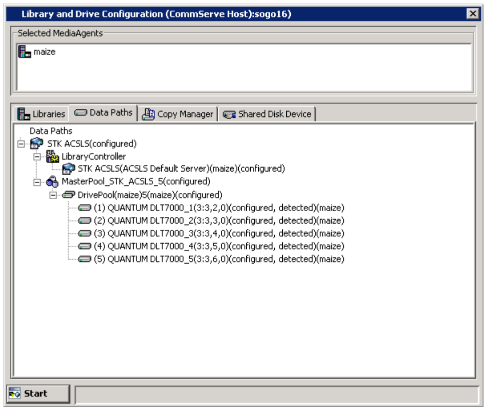
TO CONFIGURE A STORAGETEK LIBRARY WITH DDS

1. Display the Library and Drive Configuration window.

2. In the **Select MediaAgents** dialog box, select the name of the MediaAgent in which you have installed either the StorageTek's *Library Attach for Windows*,or the ACSLS Client Service for Solaris.

3. Follow steps in Direct-attached Library Configuration (with or without SN6000) to configure the library and drives in the primary MediaAgent.

Once the library is configured, the **Library and Drive Configuration** window will display a setup similar to the following:



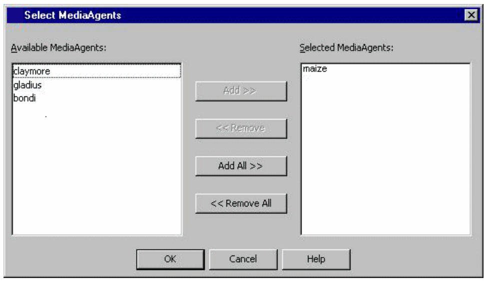
maize

```
Data Paths
STK ACSLS(configured)
  LibraryController
    STK ACSLS(ACSLS Default Server)(maize)(configured)
  MasterPool_STK_ACSLS_5(configured)
    DrivePool(maize)5(maize)(configured)
      (1) QUANTUM DLT7000_1(3:3,2,0)(configured, detected)(maize)
      (2) QUANTUM DLT7000_2(3:3,3,0)(configured, detected)(maize)
      (3) QUANTUM DLT7000_3(3:3,4,0)(configured, detected)(maize)
      (4) QUANTUM DLT7000_4(3:3,5,0)(configured, detected)(maize)
      (5) QUANTUM DLT7000_5(3:3,6,0)(configured, detected)(maize)
```

4. From the `Library and Drive Configuration` window, click the **Start** menu and choose **Select MediaAgents**.

Select the following MediaAgents:

- The MediaAgent in which the library is already configured.
- Another MediaAgent in which you wish to configure the library using DDS.



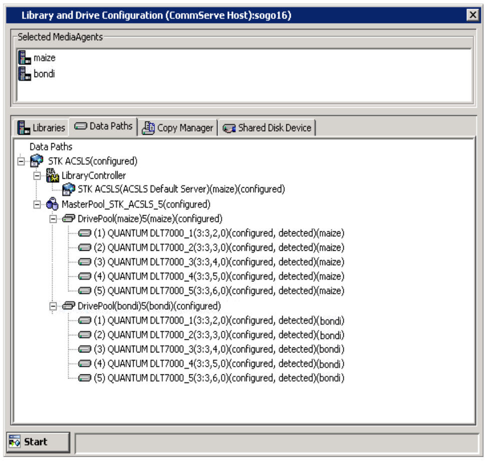
Available MediaAgents: claymore, gladius, bondi

Selected MediaAgents: maize

5. Detect the devices that are controlled by MediaAgents that will access the library as described in Detect Devices.

Exhaustive detection operation does not provide any additional advantage on StorageTek libraries using ACSLS server.

6. The system detects the drives and automatically displays them with the DDS setup in the **Library and Drive Configuration** window.



```
Data Paths
STK ACSLS(configured)
    LibraryController
        STK ACSLS(ACSLS Default Server)(maize)(configured)
    MasterPool_STK_ACSLS_5(configured)
        DrivePool(maize)5(maize)(configured)
            (1) QUANTUM DLT7000_1(3:3,2,0)(configured, detected)(maize)
            (2) QUANTUM DLT7000_2(3:3,3,0)(configured, detected)(maize)
            (3) QUANTUM DLT7000_3(3:3,4,0)(configured, detected)(maize)
            (4) QUANTUM DLT7000_4(3:3,5,0)(configured, detected)(maize)
            (5) QUANTUM DLT7000_5(3:3,6,0)(configured, detected)(maize)
        DrivePool(bondi)5(bondi)(configured)
            (1) QUANTUM DLT7000_1(3:3,2,0)(configured, detected)(bondi)
            (2) QUANTUM DLT7000_2(3:3,3,0)(configured, detected)(bondi)
            (3) QUANTUM DLT7000_3(3:3,4,0)(configured, detected)(bondi)
            (4) QUANTUM DLT7000_4(3:3,5,0)(configured, detected)(bondi)
            (5) QUANTUM DLT7000_5(3:3,6,0)(configured, detected)(bondi)
```

7. Configure the Master Drive Pool. Make sure that the drive pool and drives are configured.
8. Repeat this procedure to configure another MediaAgent in the DDS setup.

POST CONFIGURATION CONSIDERATIONS

- If you have multiple mail slots in the library, you must specify the CAP ID associated with the mail slot that will be used for importing and exporting media. (See Specify the CAP ID for Importing and Exporting Media for step-by-step instructions.)
- If you have configured a library using SN6000, it is recommended that you allocate the number of drives in the Drive Allocation Policy to the number of physical drives in the library. For example, if you have 5 physical drives in the library, and you have virtualized it using SN6000 to 10 drives, set the number of drives in the Drive Allocation Policy to 5. For step-by-step instructions on how to allocate drives in a drive allocation policy, see Set the Maximum Number of Drives for each Drive Pool in a Master Drive Pool.

CONFIGURING STK LIBRARIES WITH MULTIPLE LSMS

The following procedure describes the steps involved in configuring the STK libraries with multiple LSMs attached to the ACSLS Server using the **Library and Drive Configuration** window.

Due to the unique nature of this library, the goal of this configuration is to eliminate the sharing of resources across LSMs. In order to do this, each LSM is configured as a logical library. The following procedure describes the steps involved in configuring a LSM as a virtual library. Repeat this procedure to configure all the LSMs in the library.

BEFORE YOU BEGIN

PRE-CONFIGURATION TASKS IN THE ACSLS SERVER COMPUTER

Perform the following tasks in the ACSLS Server computer in which the library controller will be configured:

- Ensure that the hardware is configured according to the guidelines provided in Hardware Configuration Guidelines - STK Libraries Attached to ACSLS Server.
- Verify that the ACSLS server is online and the STK library is functioning.

  NOTES

  See the STK/ACSLS documentation for instructions on verifying the status of the ACSLS Server/STK library.
- In the ACSLS server, create a scratch pool for each LSM. Ensure that all volumes moved into each scratch pool reside in their respective LSMs.

  NOTES

  See the STK/ACSLS documentation for instructions on creating the scratch pool and moving the tapes to the scratch pool.

PRE-CONFIGURATION TASKS IN THE MEDIAAGENT COMPUTER

- Ensure that the hardware is configured according to the guidelines provided in ACSLS Library Configuration.
- Install one of the following, depending on the MediaAgent's Operating System:

  For a Windows MediaAgent, install an instance of StorageTek's *Library Attach for Windows* on the computer in which the MediaAgent will be installed.

  NOTES

  See the STK/ACSLS documentation for instructions on installing the *Library Attach for Windows*.
- For a Solaris MediaAgent, install the ACSLS Client Service. This service can be installed in one of the following ways:
  - During the MediaAgent software installation on the Solaris computer. See Install the MediaAgent - Solaris for step-by-step instructions on installing the MediaAgent software on Solaris.
  - If you have already installed the MediaAgent, you can run the `config_acsls` program on the Solaris MediaAgent computer. See Install ACSLS Client Service on Solaris for step-by-step instructions .

- As each LSM is configured as a library, verify that you have sufficient `Library Control Module` licenses available in the CommServe.
- This feature requires a Feature License to be available in the CommServe® Server.

  Review general license requirements included in License Administration. Also, View All Licenses provides step-by-step instructions on how to view the license information.

Required Capability: See Capabilities and Permitted Actions

TO CONFIGURE A STORAGETEK LIBRARY USING ACSLS SERVER (DIRECT-ATTACHED LIBRARY OR SAN-DDS CONFIGURATION)

1. Display the Library and Drive Configuration window.

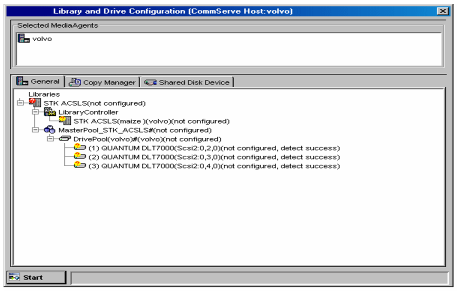
You cannot configure a StorageTek library attached to ACSLS server from the **Library and Drive Configuration** window displayed during the MediaAgent installation.

2. Detect the devices as described in Detect Devices.

Do not perform an Exhaustive Detection now.

The devices are displayed in the library tree with detection status `not configured`, `detect success` in the **Library and Drive Configuration** window.

If the system detects the drives and displays them as a standalone library in the **Library and Drive Configuration** window, perform the steps described in Configuring Drives Displayed as Stand-Alone Drives.



volvo

Libraries
STK ACSLS(not configured)
LibraryController
STK ACSLS(maize)(volvo)(not configured)
MasterPool_STK_ACSLS#(not configured)
DrivePool(volvo)#(volvo)(not configured)
(1) QUANTUM DLT7000(Scsi2:0,2,0)(not configured, detect success)
(2) QUANTUM DLT7000(Scsi2:0,3,0)(not configured, detect success)
(3) QUANTUM DLT7000(Scsi2:0,4,0)(not configured, detect success)

3. If you want to modify the library properties, right-click the library and select **Properties**.

From the **Library Properties** dialog box, you can change the following properties:

Alias: The user-defined name for the library. This name is displayed in the CommCell Console for the library. We recommend that you give each library a descriptive name as its Alias, for easier system administration.

4. When you are satisfied with your changes, click **OK**.

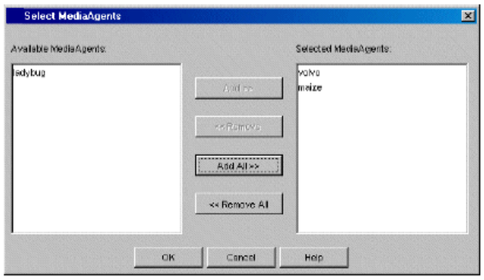
5. Configure the library as described in Configure Devices.

PERFORM THE FOLLOWING STEPS, IF YOU ARE CONFIGURING THE LIBRARY WITH DDS

6. From the **Library and Drive Configuration** window, click the **Start** menu and choose **Select MediaAgents**.

Select the following MediaAgents:

- The MediaAgent in which the library is already configured.
- Another MediaAgent in which you wish to configure the library using DDS.



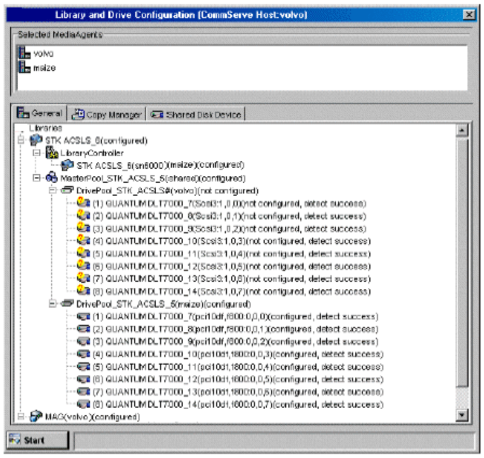
ladybug

volvo
maize

7. Detect the devices that are controlled by MediaAgents that will access the library as described in Detect Devices.

Exhaustive detection operation does not provide any additional advantage on StorageTek libraries using ACSLS server.

8. The system detects the drives and automatically displays them with the DDS setup in the **Library and Drive Configuration** window.



```
volvo
msize

Libraries
STK ACSLS_6(configured)
    LibraryController
        STK ACSLS_6(sn6000)(msize)(configured)
    MasterPool_STK_ACSLS_5(shared)(configured)
        DrivePool_STK_ACSLS#(volvo)(not configured)
            (1) QUANTUM DLT7000_7(Scsi3:1,0,0)(not configured, detect success)
            (2) QUANTUM DLT7000_8(Scsi3:1,0,1)(not configured, detect success)
            (3) QUANTUM DLT7000_9(Scsi3:1,0,2)(not configured, detect success)
            (4) QUANTUM DLT7000_10(Scsi3:1,0,3)(not configured, detect success)
            (5) QUANTUM DLT7000_11(Scsi3:1,0,4)(not configured, detect success)
            (6) QUANTUM DLT7000_12(Scsi3:1,0,5)(not configured, detect success)
            (7) QUANTUM DLT7000_13(Scsi3:1,0,6)(not configured, detect success)
            (8) QUANTUM DLT7000_14(Scsi3:1,0,7)(not configured, detect success)
        DrivePool_STK_ACSLS_5(msize)(configured)
            (1) QUANTUM DLT7000_7(pci10df,f800:0,0,0)(configured, detect success)
            (2) QUANTUM DLT7000_8(pci10df,f800:0,0,1)(configured, detect success)
            (3) QUANTUM DLT7000_9(pci10df,f800:0,0,2)(configured, detect success)
            (4) QUANTUM DLT7000_10(pci10d1,1800:0,0,3)(configured, detect success)
            (5) QUANTUM DLT7000_11(pci10d1,1800:0,0,4)(configured, detect success)
            (6) QUANTUM DLT7000_12(pci10d1,1800:0,0,5)(configured, detect success)
            (7) QUANTUM DLT7000_13(pci10d1,1800:0,0,6)(configured, detect success)
            (8) QUANTUM DLT7000_14(pci10d1,1800:0,0,7)(configured, detect success)
MAG(volvo)(configured)
```

9. Configure the Master Drive Pool. Make sure that the drive pool and drives are configured.
10. Repeat steps 6 to 10 to configure another MediaAgent in the DDS setup.

POST-CONFIGURATION CONSIDERATIONS

Consider the following after configuring all the LSMs as a virtual library:

CREATING STORAGE POLICIES

Recommended Method

When a library is configured, the system automatically creates a storage policy. In the case of libraries with multiple LSMs, a storage policy will be created for each of the LSMs configured as a library.

- Use one of these storage policies and associate all the subclients using the library to this storage policy.
- Add the data paths for each LSM in the library as alternate data paths in this storage policy. A data path for each LSM implies all possible MediaAgents that have visibility to the drives in that LSM. (Review Alternate Data Paths (GridStor) for additional information. Also, Configure Multiple Data Paths for a Storage Policy Copy provides step-by-step instructions on how to configure alternate data paths.)

The advantages to this configuration method is that when there is failure in any one of the LSMs , data protection operations will automatically use the resources in the other LSM. Thus this configuration minimizes the impact of a robot failure in any one of the LSMs. In addition only one storage policy must be configured (and maintained) resulting in easier administration.

Note that data may get scattered across several tape cartridges within the library. However, the system can keep track of all the data and automatically restore data from the appropriate tape cartridge. In addition the MediaAgent software provides several methods to reconsolidate the data. This is discussed in the Best Practices section for Alternate Data Paths (GridStor).

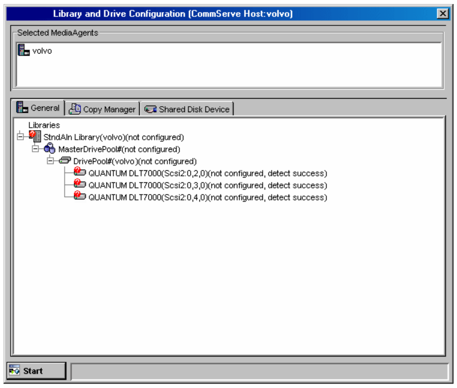
Other Methods

- Configure all the storage policies associated with each of the LSMs with alternate data paths in each of these storage policies. These alternate data paths must point to all other MediaAgents that have visibility to the drives in that LSM. Make sure to set the criteria for selecting alternate data paths as **When resources are busy or offline**. (**Load balance (Spill and fill) between Data Paths** is applicable only in the case of load balancing.) The advantage to this method is that data associated with each storage policy will be limited to the LSM to which the storage policy is associated. (Data is less scattered than in the previous method.)

  However, keep in mind that you must configure and maintain multiple storage policies in this method.
- Configure all the storage policies associated with each of the LSMs with no alternate data paths. The disadvantage here is that when one LSM fails, all backups to that LSM would fail.
- If you have multiple mail slots in the library, you must specify the CAP ID associated with the mail slot that will be used for importing and exporting media. (See Specify the CAP ID for Importing and Exporting Media for step-by-step instructions.)
- If you have mixed drive types in a LSM, consider the guidelines provided for Libraries with Mixed Drive Types.

CONFIGURING DRIVES DISPLAYED AS STAND-ALONE DRIVES

Perform the following steps if the system detects the drives and displays them as a standalone library in the **Library and Drive Configuration** window, as shown in the sample image.

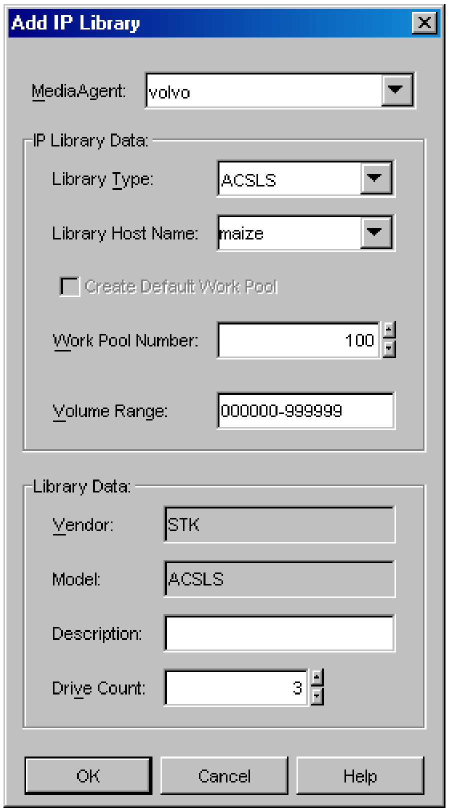


Library and Drive Configuration (CommServe Host:volvo)

Selected MediaAgents: volvo

```
Libraries
StndAln Library(volvo)(not configured)
  MasterDrivePool#(not configured)
    DrivePool#(volvo)(not configured)
      QUANTUM DLT7000(Scsi2:0,2,0)(not configured, detect success)
      QUANTUM DLT7000(Scsi2:0,3,0)(not configured, detect success)
      QUANTUM DLT7000(Scsi2:0,4,0)(not configured, detect success)
```

From the **Library and Drive Configuration** window, click the **Start** menu, choose **Add** and then select **IP Library** from the shortcut menu.



Add IP Library

MediaAgent: volvo

IP Library Data:

Library Type: ACSLS

Library Host Name: maize

□ Create Default Work Pool

Work Pool Number: 100

Volume Range: 000000-999999

Library Data:

Vendor: STK

Model: ACSLS

Description:

Drive Count: 3

In the **Add IP Library** dialog box, enter/select the following information:

MediaAgent: The name of the MediaAgent controlling the library.

Library Type: The IP library type. (ACSLS)

Library Host Name: The host name of the ACSLS server. If you have SN6000 attached, the host name of SN6000.

Work Pool Number: The work pool number associated with the work pool created for the system in the ACSLS server.

As we are configuring a library for each LSM, make sure to specify the appropriate work pool number associated with the LSM.

Volume Range: The ascending barcode range(s) of volumes available in the specified work pool. Use a dash to specify range and commas to delimit ranges. For example: 000065-000165,000167,000170-000199.

Vendor: The manufacturer of the library. (STK)

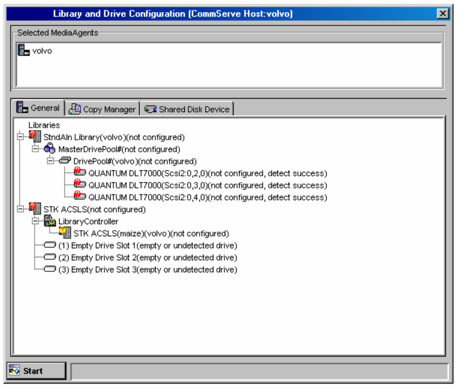
Model: The library model. (ACSLS)

Description: An optional field into which you can enter a description for the library

Drive Count: The number of drives in the library.

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

The system detects the library and displays the library information in the **Library and Drive Configuration** window.

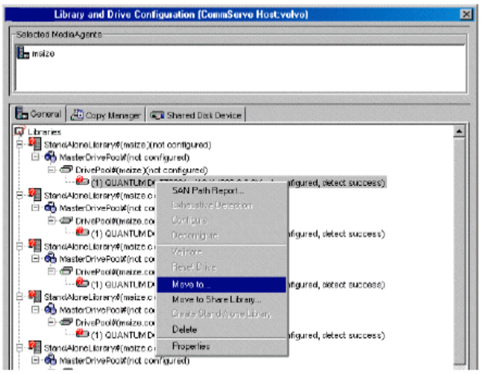


Library and Drive Configuration (CommServe Host:volvo)

Selected MediaAgents: volvo

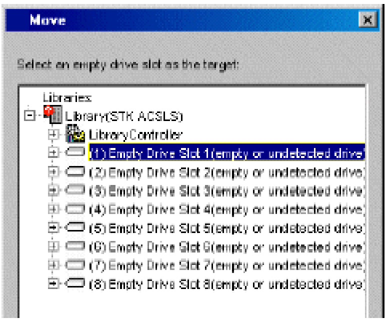
```
Libraries
StndAln Library(volvo)(not configured)
  MasterDrivePool#(not configured)
    DrivePool#(volvo)(not configured)
      QUANTUM DLT7000(Scsi2:0,2,0)(not configured, detect success)
      QUANTUM DLT7000(Scsi2:0,3,0)(not configured, detect success)
      QUANTUM DLT7000(Scsi2:0,4,0)(not configured, detect success)
STK ACSLS(not configured)
  LibraryController
    STK ACSLS(maize)(volvo)(not configured)
  (1) Empty Drive Slot 1(empty or undetected drive)
  (2) Empty Drive Slot 2(empty or undetected drive)
  (3) Empty Drive Slot 3(empty or undetected drive)
```

Right-click a stand-alone drive and choose the **Move To** option.



Libraries
StandAloneLibrary#(maize)(not configured)
MasterDrivePool#(not configured)
DrivePool#(maize)(not configured)
(1) QUANTUM D… figured, detect success)
StandAloneLibrary#(maize.c…
MasterDrivePool#(not co…
DrivePool#(maize.co…
(1) QUANTUM D… figured, detect success)
StandAloneLibrary#(maize.c…
MasterDrivePool#(not co…
DrivePool#(maize.co…
(1) QUANTUM D… figured, detect success)
StandAloneLibrary#(maize.c…
MasterDrivePool#(not co…
DrivePool#(maize.co…
(1) QUANTUM D… figured, detect success)
StandAloneLibrary#(maize.c…
MasterDrivePool#(not configured)

In the **Move to the Empty Drive Slot** dialog box click the drive number to which you wish to move the standalone drive.



Select an empty drive slot as the target:

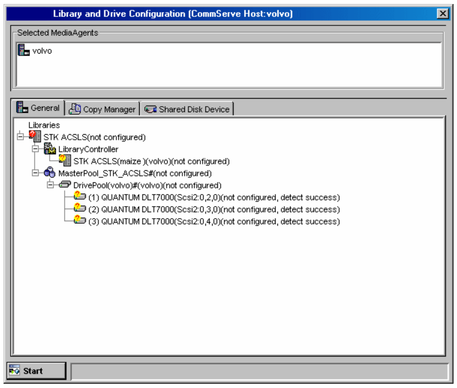
Libraries
Library(STK ACSLS)
LibraryController
(1) Empty Drive Slot 1(empty or undetected drive)
(2) Empty Drive Slot 2(empty or undetected drive)
(3) Empty Drive Slot 3(empty or undetected drive)
(4) Empty Drive Slot 4(empty or undetected drive)
(5) Empty Drive Slot 5(empty or undetected drive)
(6) Empty Drive Slot 6(empty or undetected drive)
(7) Empty Drive Slot 7(empty or undetected drive)
(8) Empty Drive Slot 8(empty or undetected drive)

Click **OK**.

Click **Yes** in the confirmation prompt for moving the drive to the empty slot.

Repeat steps 8 to 11 to move all other associated stand-alone drives to the appropriate drive slots in the library tree.

The devices are displayed in the library tree with detection status `not configured, detect success` in the **Library and Drive Configuration** window.



Libraries
STK ACSLS(not configured)
LibraryController
STK ACSLS(maize)(volvo)(not configured)
MasterPool_STK_ACSLS#(not configured)
DrivePool(volvo)#(volvo)(not configured)
(1) QUANTUM DLT7000(Scsi2:0,2,0)(not configured, detect success)
(2) QUANTUM DLT7000(Scsi2:0,3,0)(not configured, detect success)
(3) QUANTUM DLT7000(Scsi2:0,4,0)(not configured, detect success)

Right-click the drive and then click **Properties**.

In the **Drive Properties** dialog box, select the correct **ACSLS Drive ID** to match the **Serial Number** of the physical drive in the library.

Verify the drive serial number and obtain the corresponding drive ID, before selecting the drive ID in this dialog box.

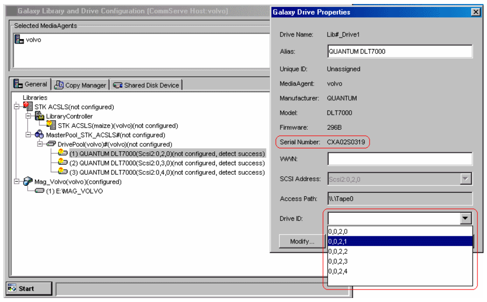
To assist in this mapping operation, use the following ACSLS command on the ACSLS server to map the **Serial Number to the ACSLS Drive ID**:

To obtain the serial number of a specific drive:

```
display drive <ACSLS Drive ID> -f serial_num
```

To obtain the serial number of all drives:

```
display drive * -f serial_num
```



Libraries
STK ACSLS(not configured)
LibraryController
STK ACSLS(maize)(volvo)(not configured)
MasterPool_STK_ACSLS#(not configured)
DrivePool(volvo)#(volvo)(not configured)
(1) QUANTUM DLT7000(Scsi2:0,2,0)(not configured, detect success)
(2) QUANTUM DLT7000(Scsi2:0,3,0)(not configured, detect success)
(3) QUANTUM DLT7000(Scsi2:0,4,0)(not configured, detect success)
Mag_Volvo(volvo)(configured)
(1) E:\MAG_VOLVO

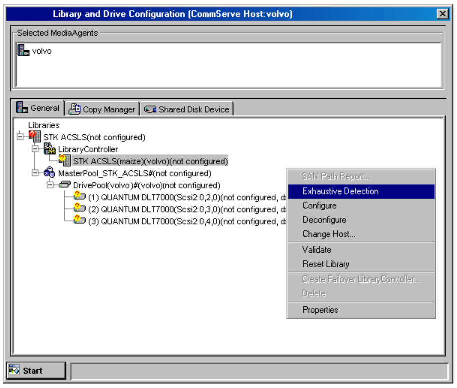
Drive Name: Lib#_Drive1
Alias: QUANTUM DLT7000
Unique ID: Unassigned
MediaAgent: volvo
Manufacturer: QUANTUM
Model: DLT7000
Firmware: 296B
Serial Number: CXA02S0319
WWN:
SCSI Address: Scsi2:0,2,0
Access Path: \\.\Tape0
Drive ID:
0,0,2,0
0,0,2,1
0,0,2,2
0,0,2,3
0,0,2,4

If the list of the ACSLS drive IDs is not populated, verify and ensure that the ACSLS Client Service is running.

Repeat steps 14 to 15 for all the drives within each LSM in the library.

If you are not sure of the drive serial number and drive ID mapping, then perform an exhaustive detection of the devices at the Library Controller level.

This will ensure that the drives are mapped to the appropriate serial number.

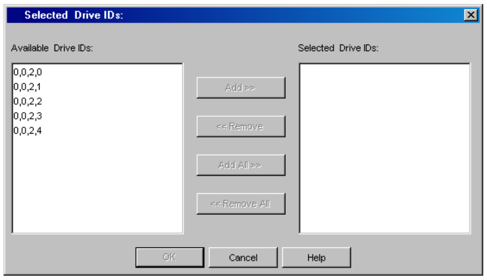


Library and Drive Configuration (CommServe Host:volvo)
Selected MediaAgents
volvo
General
Copy Manager
Shared Disk Device
Libraries
STK ACSLS(not configured)
LibraryController
STK ACSLS(maize)(volvo)(not configured)
MasterPool_STK_ACSLS#(not configured)
DrivePool(volvo)#(volvo)(not configured)
(1) QUANTUM DLT7000(Scsi2:0,2,0)(not configured, d
(2) QUANTUM DLT7000(Scsi2:0,3,0)(not configured, d
(3) QUANTUM DLT7000(Scsi2:0,4,0)(not configured, d
SAN Path Report...
Exhaustive Detection
Configure
Deconfigure
Change Host...
Validate
Reset Library
Create Failover LibraryController...
Delete
Properties
Start

Select the most likely drives or all the available drives in the **Select Drive IDs** dialog box.

NOTES

As this process attempts to mount a media in each of the selected drives to determine the drive numbers to its correct serial number, depending on the number of drives selected, this operation may take several minutes to complete.



Proceed to Step 3.

STK Libraries Attached to ACSLS Server - How To

Topics | Configure | How To | Related Topics

Add Volume Ranges

Specify the CAP ID for Importing and Exporting Media

Move a Media using the Set Scratch option

Install ACSLS Client Service on Solaris

Display Cleaning Media in the CommCell Console

Automatically Detect Replaced Drives

ADD VOLUME RANGES

The following procedure describes the steps for adding volume ranges.

Required Capability: See Capabilities and Permitted Actions

➡ To add volume ranges in a library attached to ACSLS server:

1. Display the Library and Drive Configuration window.
2. Right-click the library in which you wish to add the volume ranges and then click **Properties**.
3. From the Library Properties dialog box, enter the complete list of barcode ranges for volumes (tapes) in the library in the **Volume Range** box.
4. Click **OK** to save the details.

SPECIFY THE CAP ID FOR IMPORTING AND EXPORTING MEDIA

Use the following procedure to specify the CAP ID associated with the mail slot that will be used for importing and exporting media from the specific MediaAgent.

Required Capability: See Capabilities and Permitted Actions

➡ To specify the CAP ID for importing and exporting media:

1. From the CommCell Browser, right-click the library for which you wish to change the CAP selection, and then click **Properties**.

2. Click the CAP Selection tab.
3. Select the CAP ID that must be used for importing and exporting media.
4. Click **OK**.

MOVE A MEDIA USING THE SET SCRATCH OPTION

Required Capability: See Capabilities and Permitted Actions

To move a media using the Set Scratch option in a library attached to ACSLS server:

1. From the CommCell Console navigate to the Exported Media pool in the library in which the media resides.
2. From the right-pane, right-click the media and click **Set Scratch** and then select the scratch pool to which you wish to move the media.
3. Click **OK** to save the details.

INSTALL ACSLS CLIENT SERVICE ON SOLARIS

On a Solaris MediaAgent, the ACSLS Client Service must be installed before configuring the STK library attached to an ACSLS Server. You can install the ACSLS service when you install the Solaris MediaAgent. However, if you have already installed the Solaris MediaAgent and wish to configure a STK library controlled by an ACSLS server, you can use the `Config ACSLS Services` package to add the necessary services.

The following procedure describes the steps involved in installing the ACSLS Service using the `Config ACSLS Services` package.

1. Log on to the MediaAgent computer as `root`.
2. Run the following program:

   ```
   <software installation path>/Base/config_acsls
   ```

3. The following menu is displayed if ACSLS services are not configured:

   ```
   Please select one of the options below:

   1) Config ACSLS Services

   2) Exit

   Your selection: [2]
   ```

   Type `1` and then press **Enter**.

4. The following prompt is displayed:

   ```
   Please enter the name of the host running the ACSLS daemon. ACSLS Server host name:
   ```

   Enter the name of the host in which the ACSLS server is installed and then press `Enter`.

   or

   If you are accessing the library using SN6000, enter the host name of SN6000 and then press `Enter`.

   The system copies the necessary files and creates the necessary configuration and displays the following message:

   ```
   ACSLS services are currently CONFIGURED.
   ```

5. The menu is displayed.

   Enter the number corresponding to the `Exit` option to exit the package.

Use the `Calypso list` command to check if the SSI service is running on the Solaris computer. See Service Control for Unix for details.

POST-INSTALL CONSIDERATIONS

Perform the following steps if the MediaAgent communicates with the ACSLS Server across a firewall:

1. Make sure the Firewall Secure option is configured in ACSLS Server and get the CSI_INET_PORT number.
2. Edit the `ssi.env` file in the `Base` directory and add the following script below the line for `ACSAPI_SSI_SOCKET=40004` setting and replace the `SSI_HOSTNAME` and two port numbers, if the values are different:

   ```
   ## additional parameters for ACSLS client firewall setting

   # add Client side SSI_HOSTNAME - hardcoded now ; SSI_INET_PORT=30031 (default)

   SSI_HOSTNAME=; export SSI_HOSTNAME
   ```

```
SSI_INET_PORT=30031; export SSI_INET_PORT

# add Server CSI_HOSTPORT=30031 (default) - must match CSI_INET_PORT setting on ACSLS Server

CSI_HOSTPORT=30031; export CSI_HOSTPORT

# trun off UDP protocol CSI_UDP_RPCSERVICE="FALSE"; export CSI_UDP_RPCSERVICE

## End firewall setting
```

3. Stop and start the services. (See Stop Services on Unix and Start Services on Unix for step-by-step instructions.)
4. Verify communication between the MediaAgent and the ACSLS Server by running `the ACSLSTool` available in the `Base` directory.

DISPLAY CLEANING MEDIA IN THE COMMCELL CONSOLE

1. Display the Library and Drive Configuration window.
2. Right-click the library in which you wish to add the volume ranges and then click **Properties**.
3. From the Library Properties dialog box, select the **List ACSLS Clean Media** option.
4. Click **OK** to save the details.
5. Right click the library and then click **Reset Library**.

   Once the library is reset, media containing the characters CLN as the first three characters in its barcode will be displayed in the **Media in Library** pool in the CommCell Console.

AUTOMATICALLY DETECT REPLACED DRIVES

1. Display the Library and Drive Configuration window.
2. Right-click the library in which you wish to add the volume ranges and then click **Properties**.
3. From the Library Properties dialog box, select the **Use Drive ID for Drive Replacement** option.
4. Click **OK** to save the details.

Back to Top

ADIC Libraries Attached to Scalar Distributed Library Controller (SDLC)

Topics | Configure | Related Topics

OVERVIEW

The system supports the configuration of one or more Windows MediaAgents in a CommCell, connecting directly to a number of drives in a ADIC library controlled by the Scalar Distributed Library Controller (SDLC).

Such libraries can be shared between:

- Multiple MediaAgents in a CommCell
- Multiple CommCells, or
- CommCells and others applications

Note that the SDLC server computer can also be a component (either a MediaAgent or an agent) of the CommCell.

Once configured, all library related operations are supported. (For more information on the supported operations, see Library Operations, Drive Operations and Media Operations.)

ADIC Libraries Attached to Scalar Distributed Library Controller (SDLC) - Configure

Topics | Configure | Related Topics

Within a CommCell, depending on the environment, the MediaAgents can be configured to access the ADIC library controlled by SDLC using one of the following configurations:

- Direct-attached library configuration
- Dynamic Drive Sharing (DDS) configuration in the SAN environment

The following procedure describes the steps involved in configuring the ADIC library attached to SDLC as a direct attached library using the **Library and Drive Configuration** window.

BEFORE YOU BEGIN

PRE-CONFIGURATION TASKS IN THE SDLC COMPUTER

- Ensure that the hardware is configured according to the guidelines provided in ADIC Libraries Attached to Scalar Distributed Library Controller (SDLC) Configuration.
- Verify that the SDLC is online and the ADIC library is functioning. See the SDLC documentation for instructions on verifying the status of the SDLC/ADIC library.
- If the library is shared between multiple CommCells or applications, define the necessary Volume Range for the exclusive use of the CommCell to which the MediaAgent(s) you wish to configure are attached. See the SDLC documentation for instructions on creating the volume ranges.

PRE-CONFIGURATION TASKS IN THE MEDIAAGENT COMPUTER

- Ensure that the hardware is configured according to the guidelines provided in ADIC Libraries Attached to Scalar Distributed.
- Install the DAS Client software on the MediaAgent computer. See the DAS Client documentation for more information.
- This feature requires a Feature License to be available in the CommServe® Server.

  Review general license requirements included in License Administration. Also, View All Licenses provides step-by-step instructions on how to view the license information.

Required Capability: See Capabilities and Permitted Actions

TO CONFIGURE A ADIC LIBRARIES ATTACHED TO SDLC

1. Display the Library and Drive Configuration window.

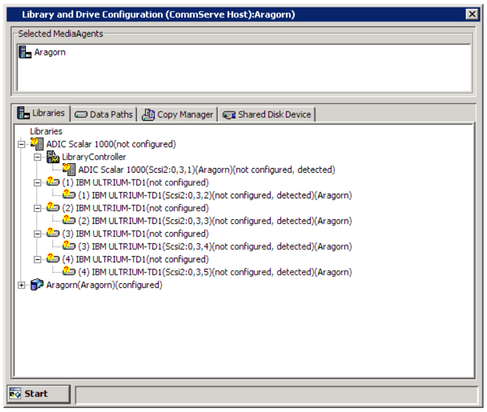
You cannot configure a ADIC library attached to SDLC from the **Library and Drive Configuration** window displayed during the MediaAgent installation.

2. Detect the devices as described in Detect Devices.

   Do not perform an Exhaustive Detection now.

   The system detects the drives and displays them as a standalone library in the **Library and Drive Configuration** window.

   If the library supports Drive Serialization, then the drives would be detected as ADIC Scalar library. The sample image shows the drives detected as ADIC Scalar library.



```
Libraries
ADIC Scalar 1000(not configured)
  LibraryController
    ADIC Scalar 1000(Scsi2:0,3,1)(Aragorn)(not configured, detected)
  (1) IBM ULTRIUM-TD1(not configured)
    (1) IBM ULTRIUM-TD1(Scsi2:0,3,2)(not configured, detected)(Aragorn)
  (2) IBM ULTRIUM-TD1(not configured)
    (2) IBM ULTRIUM-TD1(Scsi2:0,3,3)(not configured, detected)(Aragorn)
  (3) IBM ULTRIUM-TD1(not configured)
    (3) IBM ULTRIUM-TD1(Scsi2:0,3,4)(not configured, detected)(Aragorn)
  (4) IBM ULTRIUM-TD1(not configured)
    (4) IBM ULTRIUM-TD1(Scsi2:0,3,5)(not configured, detected)(Aragorn)
Aragorn(Aragorn)(configured)
```

3. From the **Library and Drive Configuration** window, click the **Start** menu, choose **Add** and then select **IP Library** from the shortcut menu.

4. In the **Add Library** dialog box, enter/select the following information:

   MediaAgent: The name of the MediaAgent.

   Library Type: The IP library type. (ADIC)

   Library Host Name: The name of the MediaAgent where the drives are currently configured. (This is also the DAS Client.)

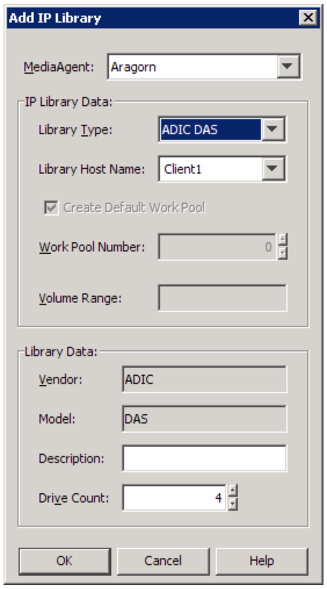
   Vendor: The manufacturer of the library.

   Model: The library model.

   Description: An optional field into which you can enter a description for the library

   Drive Count: The number of drives in the library.

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



MediaAgent: Aragorn

Library Type: ADIC DAS

Library Host Name: Client1

☑ Create Default Work Pool

Work Pool Number: 0

Volume Range:

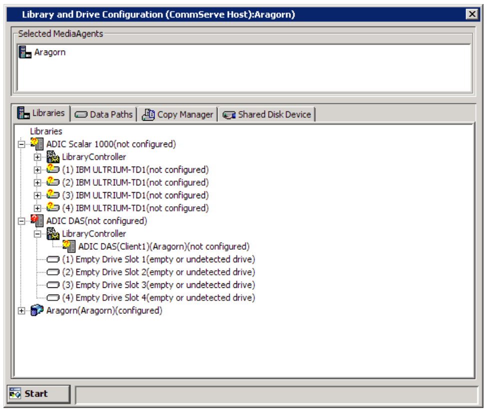
Vendor: ADIC

Model: DAS

Description:

Drive Count: 4

The system detects the library and displays the library information in the **Library and Drive Configuration** window.



```
Libraries
ADIC Scalar 1000(not configured)
  LibraryController
  (1) IBM ULTRIUM-TD1(not configured)
  (2) IBM ULTRIUM-TD1(not configured)
  (3) IBM ULTRIUM-TD1(not configured)
  (4) IBM ULTRIUM-TD1(not configured)
ADIC DAS(not configured)
  LibraryController
    ADIC DAS(Client1)(Aragorn)(not configured)
  (1) Empty Drive Slot 1(empty or undetected drive)
  (2) Empty Drive Slot 2(empty or undetected drive)
  (3) Empty Drive Slot 3(empty or undetected drive)
  (4) Empty Drive Slot 4(empty or undetected drive)
Aragorn(Aragorn)(configured)
```

5. If you want to modify the library properties, right-click the library and select **Properties**.

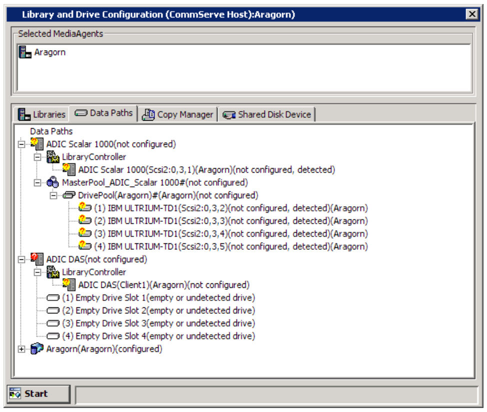
   From the **Library Properties** dialog box, you can change the following properties:

   Alias: The user-defined name for the library. This name is displayed in the CommCell Console for the library. We recommend that you give each library a descriptive name as its Alias, for easier system administration.

   When you are satisfied with your changes, click **OK.**

6. Highlight the **MasterPool** from the detected library and then drag and drop it on the `ADIC DAS` library.

The devices are displayed in the library tree with detection status `not configured, detect success` in the `Library and Drive Configuration` window.

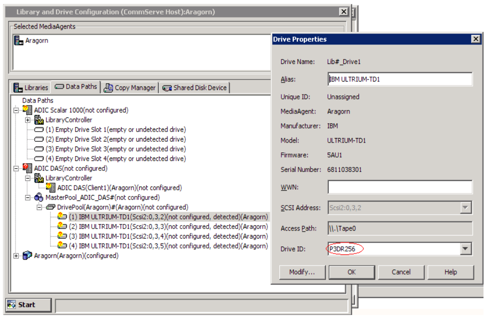


```
Data Paths
ADIC Scalar 1000(not configured)
  LibraryController
    ADIC Scalar 1000(Scsi2:0,3,1)(Aragorn)(not configured, detected)
  MasterPool_ADIC_Scalar 1000#(not configured)
    DrivePool(Aragorn)#(Aragorn)(not configured)
      (1) IBM ULTRIUM-TD1(Scsi2:0,3,2)(not configured, detected)(Aragorn)
      (2) IBM ULTRIUM-TD1(Scsi2:0,3,3)(not configured, detected)(Aragorn)
      (3) IBM ULTRIUM-TD1(Scsi2:0,3,4)(not configured, detected)(Aragorn)
      (4) IBM ULTRIUM-TD1(Scsi2:0,3,5)(not configured, detected)(Aragorn)
ADIC DAS(not configured)
  LibraryController
    ADIC DAS(Client1)(Aragorn)(not configured)
  (1) Empty Drive Slot 1(empty or undetected drive)
  (2) Empty Drive Slot 2(empty or undetected drive)
  (3) Empty Drive Slot 3(empty or undetected drive)
  (4) Empty Drive Slot 4(empty or undetected drive)
Aragorn(Aragorn)(configured)
```

7. Right-click the drive and then click **Properties**.

In the **Drive Properties** dialog box, select the correct drive associated with the drive ID.

Verify the drive name from the **Scalar DLC Management GUI**, before selecting the drive ID in this dialog box.



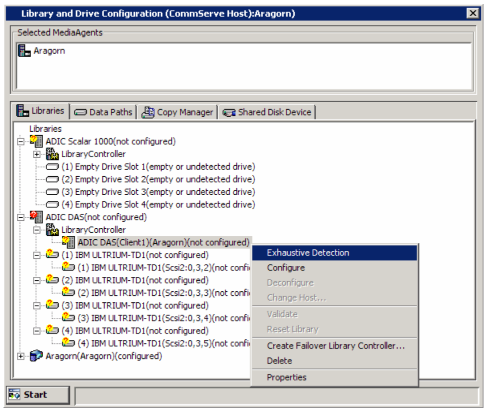
```
Data Paths
ADIC Scalar 1000(not configured)
  LibraryController
  (1) Empty Drive Slot 1(empty or undetected drive)
  (2) Empty Drive Slot 2(empty or undetected drive)
  (3) Empty Drive Slot 3(empty or undetected drive)
  (4) Empty Drive Slot 4(empty or undetected drive)
ADIC DAS(not configured)
  LibraryController
    ADIC DAS(Client1)(Aragorn)(not configured)
  MasterPool_ADIC_DAS#(not configured)
    DrivePool(Aragorn)#(Aragorn)(not configured)
      (1) IBM ULTRIUM-TD1(Scsi2:0,3,2)(not configured, detected)(Aragorn)
      (2) IBM ULTRIUM-TD1(Scsi2:0,3,3)(not configured, detected)(Aragorn)
      (3) IBM ULTRIUM-TD1(Scsi2:0,3,4)(not configured, detected)(Aragorn)
      (4) IBM ULTRIUM-TD1(Scsi2:0,3,5)(not configured, detected)(Aragorn)
Aragorn(Aragorn)(configured)
```

Drive Name: Lib#_Drive1
Alias: IBM ULTRIUM-TD1
Unique ID: Unassigned
MediaAgent: Aragorn
Manufacturer: IBM
Model: ULTRIUM-TD1
Firmware: 5AU1
Serial Number: 6811038301
WWN:
SCSI Address: Scsi2:0,3,2
Access Path: \\.\Tape0
Drive ID: P3DR256

8. Repeat steps 6 to 7 for all the drives (used by the system) in the library.

9. If you are not sure of the drive mapping, then perform an exhaustive detection of the devices from the Library Controller level.

This will ensure that the drives are mapped to the appropriate serial number.

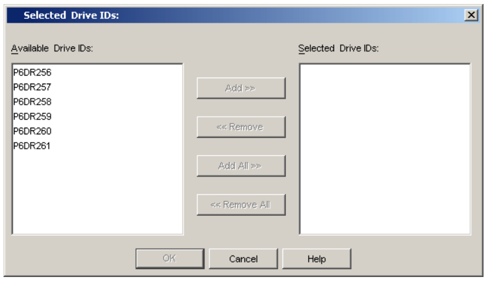


```
Libraries
ADIC Scalar 1000(not configured)
  LibraryController
  (1) Empty Drive Slot 1(empty or undetected drive)
  (2) Empty Drive Slot 2(empty or undetected drive)
  (3) Empty Drive Slot 3(empty or undetected drive)
  (4) Empty Drive Slot 4(empty or undetected drive)
ADIC DAS(not configured)
  LibraryController
    ADIC DAS(Client1)(Aragorn)(not configured)
  (1) IBM ULTRIUM-TD1(not configured)
    (1) IBM ULTRIUM-TD1(Scsi2:0,3,2)(not confi
  (2) IBM ULTRIUM-TD1(not configured)
    (2) IBM ULTRIUM-TD1(Scsi2:0,3,3)(not confi
  (3) IBM ULTRIUM-TD1(not configured)
    (3) IBM ULTRIUM-TD1(Scsi2:0,3,4)(not confi
  (4) IBM ULTRIUM-TD1(not configured)
    (4) IBM ULTRIUM-TD1(Scsi2:0,3,5)(not confi
Aragorn(Aragorn)(configured)
```

10. Select the most likely drives or all the available drives in the **Select Drive IDs** dialog box.

NOTES

As this process attempts to mount a media in each of the selected drives to determine the drive numbers to its correct serial number, depending on the number of drives selected, this operation may take several minutes to complete.



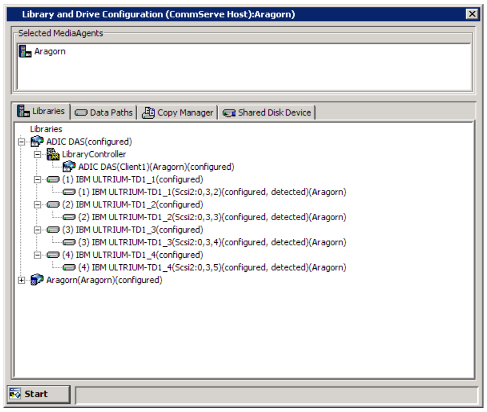
Available Drive IDs:
P6DR256
P6DR257
P6DR258
P6DR259
P6DR260
P6DR261

Selected Drive IDs:

11. Configure the library as described in Configure Devices.

The devices are displayed as `configured, detect success`.

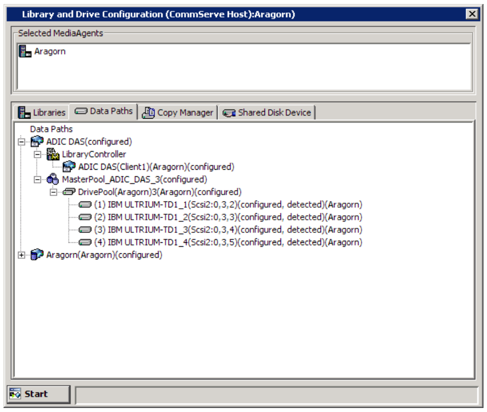
The **Library** tab provides the physical view of the devices (library and drives).



Aragorn

```
Libraries
ADIC DAS(configured)
    LibraryController
        ADIC DAS(Client1)(Aragorn)(configured)
    (1) IBM ULTRIUM-TD1_1(configured)
        (1) IBM ULTRIUM-TD1_1(Scsi2:0,3,2)(configured, detected)(Aragorn)
    (2) IBM ULTRIUM-TD1_2(configured)
        (2) IBM ULTRIUM-TD1_2(Scsi2:0,3,3)(configured, detected)(Aragorn)
    (3) IBM ULTRIUM-TD1_3(configured)
        (3) IBM ULTRIUM-TD1_3(Scsi2:0,3,4)(configured, detected)(Aragorn)
    (4) IBM ULTRIUM-TD1_4(configured)
        (4) IBM ULTRIUM-TD1_4(Scsi2:0,3,5)(configured, detected)(Aragorn)
Aragorn(Aragorn)(configured)
```

The **Data Paths** tab provides a logical view of the data path used to access the devices - library, master drive pool, drive pool, drive.



Aragorn

```
Data Paths
ADIC DAS(configured)
    LibraryController
        ADIC DAS(Client1)(Aragorn)(configured)
    MasterPool_ADIC_DAS_3(configured)
        DrivePool(Aragorn)3(Aragorn)(configured)
            (1) IBM ULTRIUM-TD1_1(Scsi2:0,3,2)(configured, detected)(Aragorn)
            (2) IBM ULTRIUM-TD1_2(Scsi2:0,3,3)(configured, detected)(Aragorn)
            (3) IBM ULTRIUM-TD1_3(Scsi2:0,3,4)(configured, detected)(Aragorn)
            (4) IBM ULTRIUM-TD1_4(Scsi2:0,3,5)(configured, detected)(Aragorn)
Aragorn(Aragorn)(configured)
```

Disk Libraries

Topics | Configure | How To | Troubleshoot | Related Topics

Disk Libraries

Overview of Disk Libraries

- Clustered File System Storage
- Automatically Create Mount Path when adding new Disk Storage

Best Practices for Disk Libraries

Shared Disk Libraries

Overview of Shared Disk Libraries

- Shared Disk libraries with Static Mount Paths
- Best Practices for Shared Disk Libraries

Disk Libraries on Replicated Disks

Overview of Disk Libraries on Replicated Disks

Common

Administering Disk Libraries

- Modify the Library Name and Description
- View the MediaAgent and the Number of Mount Paths
- View the Status
- Modify the Low Watermark
- Configure a Low Disk Space Alert
- Configure Disk Volume Size
- Configure Archive Files as Read-Only
- Configure Timeouts
- Enable Support for single instancing of Data (Content Address Storage)
- Establish the Parameters for Mount Path Usage
- Thresholds for Managed Disk Space
- Establish the Mount Path Allocation Policy for the Library
- View the storage policy and storage policy copies accessing the disk library
- Configure Security
- Migrate Disk Libraries
- Fragmentation Analysis
- Disk Volume Reconciliation
- Deconfigure a Disk Library

Administering Mount Paths

- View or modify the properties of the mount path
- Use Unbuffered I/O
- Enable or disable a mount path
- Establish the Mount Path Allocation Policy
- Establish Space Allocation on the Mount Path
- Reduce Fragmentation of Data on a Mount Path
- View the Contents of a Mount Path
- Delete the Contents of a Mount Path
- Prevent Accidentally Deleting the Contents of a Mount Path
- Moving Mount Paths
- Retire a Mount Path
- Delete a Mount Path

OVERVIEW OF DISK LIBRARIES

A disk library is a virtual library associated with one or more mount paths. The disk library does not represent a specific hardware entity; it is a software entity that contains a list of mount paths through which data can be sent to a disk media.

Disk media, whether individual hard disks or RAID arrays, is logically divided into partitions. A partition can include some or all of the total disk storage space available. Each partition is associated with a file system path called a mount path, through which data is written to and read from.

A disk library can be configured by assigning one or more mount paths to it. The storage capacity of a disk library is determined by the total storage space in its mount paths.

Note that the maximum size of a volume that can be used as a mount path can be a maximum of 4,096 Terabytes.

CLUSTERED FILE SYSTEM STORAGE

Disk libraries are supported on clustered file systems such as Global File Systems (GFS), Cluster File Systems (CFS), IBM General Parallel File System (GPFS), and Polyserve File System.

AUTOMATICALLY CREATE MOUNT PATH WHEN ADDING NEW DISK STORAGE

Automated disk library is a process to automatically add new mount paths when new LUN is mounted under given folder as Mount point. It is supported for all Windows MediaAgents.

This is useful when:

- multiple disk libraries need to be detected and automatically assign the mount paths to the library.
- storage is in Building Block and needs to be shared across MediaAgents.

See Configuring Automatic Mount Paths for New Disk Storage for step-by-step instructions.

BEST PRACTICES FOR DISK LIBRARIES

The following list provides a set of guidelines to help you ensure that the MediaAgent always accesses the mount paths allocated to disk libraries:

- You can define one or more mount paths to local or remote computers for Windows and UNIX file systems. You cannot define mount paths to a disc drive, e.g., CD-ROM drive, or a locally mapped network drive.
- Use dedicated partitions for your disk mount paths.

  We recommend the following practices while creating mount paths:

  - Do not create a mount path on the same partition in which the MediaAgent software is installed.
  - Do not create a mount path under an already existing `CV_MAGNETIC` folder.
- Make sure that each mount path contains more than 2 GB of free space when it is created, and that the total storage space in the disk library is sufficient to hold the maximum amount of data that will be stored in the library at any time.
- If you want to use a path to a remote Windows computer as a mount path, the mount path must follow the Universal Naming Convention (UNC), with the following format:

  ```
  \\<computer name>\<shared directory name>\<optional path>
  ```

  The remote computer can belong to the same domain as the MediaAgent from which it is accessed, or to a different domain, provided that a trust has been set up between that domain and the MediaAgents domain.

- When a mount path is created using UNC paths, verify and ensure that the user account used to access the mount path has sufficient permissions to read / write in the software install folder in the computer in which the MediaAgent associated with mount path is installed. This is because the MediaAgent uses these folders to create the necessary log entries in the log files for jobs associated with the mount path.
- The mount path for a disk library in a clustered environment should be a UNC path, or the shared disk on a cluster.

- An NFS mounted file system can be used as a mount path to a remote UNIX computer. The system considers an NFS mounted file system local to the computer on which it is mounted.
- The software does not permit the creation of two mount paths that access the same directory. This is true even if one mount path accesses the directory locally, while another mount path accesses it remotely.
- If the mount path directory does not exist, it is automatically created when you add the mount path.
- If a disk volume in Windows platform is found to be dirty, the volume is marked *offline*. Any attempts to access the volume will result in error. Clean up the volume and manually bring it back *online*.
- If a mount path directory is deleted or renamed (i.e., through the operating system), it is not recreated the next time a data protection operation attempts to accesses the mount path. The mount path becomes inaccessible for the job and hence the mount path is marked as *offline*. Attempts to back up to that mount path will generate error messages.

If you have defined multiple mount paths for a disk library, the system determines the specific path to which data secured by a data protection operation is written.

WRITERS AND STORAGE POLICY DATA STREAMS

The maximum number of writers for a disk library is used to determine the maximum number of simultaneous data protection operations. Hence this value is linked to the maximum number of data streams that can be established for a storage policy accessing the disk library.

Storage Policy data streams are logical channels that connect client data to the media in which data secured by data protection operations are stored. Multiple data streams can be used to parallelize an operation, in order to improve the rate at which data can be written to the media.

The practical limits for establishing data streams in a storage policy accessing a disk library is determined by the minimum value established in either the disk library or the sum of mount paths in the disk library.

The values for writers can be modified from the **Disk Library Properties** and **Mount Path Properties** dialog box available in the CommCell Console. The values for the maximum number of data streams can be modified from the **Storage Policy Properties** dialog box also available in the CommCell Console.

MANAGED DISK SPACE

For new deduplicated storage policy copies, **Enable Managed Disk Space for disk data** option on **Copy Properties** dialog box (**Retention** tab) is disabled by default. If an existing deduplication copy (for CommServe with Service Pack 8B) has this option enabled, then while updating and saving the deduplication copy, you will be asked to manually disable this option. This option will not be changed automatically for any existing deduplication copy. Disabling this option helps in faster pruning of the aged data in order to reclaim space on the disk.

For step-by-step instructions to disable **Enable Managed Disk Space for Disk Library** check box, see Enable Managed Disk Space for Disk Data.

OVERVIEW OF SHARED DISK LIBRARIES

Shared disk libraries provide the following benefits:

- Fail-over capabilities between MediaAgents
- Facility to dedicate one MediaAgents for Auxiliary Copy operations

A shared disk library supports all the operations supported (except disk migration) by a (non-shared) disk library.

SHARED DISK LIBRARIES WITH STATIC MOUNT PATHS

The concept of shared disk libraries is expanded further to include volumes that are statically mounted or accessible in a network, such as PolyServe File System, Sistina GFS (Global File systems), NFS mounted volumes or network shares. Such volumes need not be explicitly mounted and can be accessed by multiple MediaAgents at the same time.

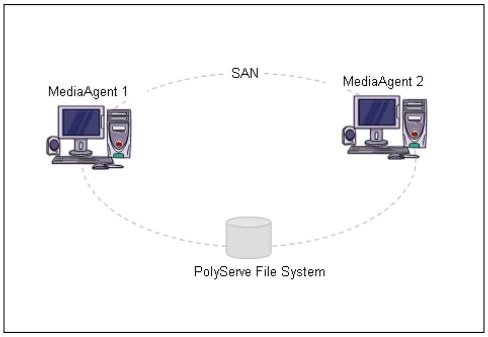
See Configure Shared Disk Libraries With Static Mount Paths for step-by-step instructions on configuring disk libraries with static mount paths.

See Configure Multiple MediaAgents for a Static Shared Disk Device for step-by-step instructions on configuring multiple MediaAgents (of same operating system type) with static shared disk devices.

CONFIGURING POLYSERVE DISKS AS STATIC MOUNT PATHS

Disks with PolyServe File System can be configured in a Storage Area Network (SAN) as a shared disk library with static mount paths, as illustrated in the diagram.

Note that when configuring such disks, use the local PolyServe exposed volume instead of using UNC paths.



See Also: MediaAgents - Supported Features, Agents and Devices for information on MediaAgents that support shared disk libraries with static mount paths

BEST PRACTICES FOR SHARED DISK LIBRARIES

The following sections provide a set of guidelines for the successful implementation of shared disk libraries.

SHARING THE SAME DISK STORAGE ACROSS MEDIAAGENTS

LAN BASED BACKUP

- For a LAN based storage access, share the disk across the servers on the LAN. The disk can be shared as CIFS or UNC, depending on the operating system of the MediaAgent computer. For concurrent access from different machines to the same volume, configure the disk library using the static shared option. (See Configure Shared Disk Libraries With Static Mount Paths for step-by-step instructions.) This configuration works well in situations where a large volume of disk space must be shared across different MediaAgents without provisioning storage for each MediaAgent separately.

LAN FREE BACKUP

- For a LAN free backup with the same LUN shared for MediaAgent failover, a cluster solution like MSCS is recommended. This will allow a seamless failover to the disk in the event of a failure on any nodes in the cluster.
- For a LAN free backup with concurrent access from multiple MediaAgents to the same disk volume at the same time, a clustered file system (e.g., PolyServe) must be configured to allow access to the same LUN from different systems. The CommCell is configured to write to the Clustered File System through static shared libraries, with sharing managed by the Clustered File System Management application.
- For a LAN free backup without the LUN sharing configuration, is recommended to configure the conventional disk libraries with each LUN presented as a dedicated storage to each MediaAgent. In the case of an MediaAgent failure, it is required to re-zone or present the LUN to another MediaAgent followed by a disk library migration, accomplished by a single task from the CommCell Console GUI. Manual intervention is only needed in the event of a MediaAgent computer failure.

MODIFYING THE ACCESS INFORMATION FOR A SHARED DISK

It may be necessary to change the access information, such as access credentials and/or path on a shared disk. For example if the access credentials is changed in the operating system you may want to set the new credentials from the CommCell Console for the disk library.

For Windows devices, you can modify the access information from the device level, which will change access information for all the MediaAgents sharing the device.

For Unix MediaAgents this must be performed from each folder level which will change the access credentials for each of the specific MediaAgents accessing the device.

See Modify the Access Information for a Shared Disk for step-by-step instructions.

OVERVIEW OF DISK LIBRARIES ON REPLICATED DISKS

For disks that are replicated to another disk in real-time using software/hardware replication tools, the mount paths from both the primary and replicated disks can be configured as a disk library. In such a configuration, the data written by the primary MediaAgent will have read-write access while the MediaAgent on the replica will have read-only access. Note that the primary and replica mount paths can be configured on any MediaAgent type (Windows, Solaris, Linux, etc) or with any network or cluster file systems. (CIFS, NTFS, etc.)

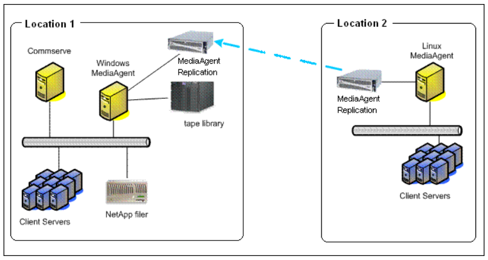
The following example illustrates a disk library configuration on a replicated disk:

In this example MediaAgent 1 is configured to access a disk library on the primary computer, to backup a mission-critical production server, such as a server with a large database. (This MediaAgent will have read-write access to the disk library on the primary.)

The data is replicated to a replica that contains MediaAgent 2. (This MediaAgent will have read access to the disk library on the replica.)

Note that when the system performs a data protection operation using the MediaAgent on the primary disk, two copies of the data are available as soon as the disk is replicated. Thus MediaAgent 2 can be used to perform auxiliary copy operations to a tape library, thus limiting the load on the processing capabilities in the production server. Also note that all data protection operations (backup and auxiliary copy) are performed LAN free.

Data can be restored from either the primary or replicated disk or from a copy using the tape library.



See Configure Disk Libraries on Replicated Disks for step-by-step- instructions on configuring such libraries.

See Disk Library Replication solution to seamlessly replicate data from remote offices to centralized data centers using disk libraries on replicated disks.

ADMINISTERING DISK LIBRARIES

There are several configurable parameters available for Disk libraries. The following sections describe each of these parameters.

MODIFY THE LIBRARY NAME AND DESCRIPTION

The system initially assigns a default name for the disk library. If necessary, you can modify the name. You can also add relevant information about the library as a description.

This operation is supported by all disk libraries.

VIEW THE MEDIAAGENT AND THE NUMBER OF MOUNT PATHS

You can view the MediaAgent name and the number of mount paths associated with each Disk library.

This operation is supported by all disk libraries.

VIEW THE STATUS

The status of the disk library indicates whether the library is online or offline, and if offline, the reason for the offline status.

You can use the enable/disable indicator to logically enable or disable the disk library.

This operation is supported by all disk libraries.

See Enable or Disable the Disk Library and View the Disk Library Offline Reason for step-by-step instructions.

MODIFY THE LOW WATERMARK

You can establish a low watermark for each disk library. The low watermark is the minimum amount of free space at which the low watermark warning should be generated. If the amount of free space, for all the combined mount paths, reaches or falls below the low watermark, the system logs a message in the Event Viewer and generates the *Insufficient Storage* Alert, if configured. See Establish the Low Watermark for a Disk Library for step-by-step instructions.

This operation is supported by all disk libraries.

CONFIGURE A LOW DISK SPACE ALERT

By default, low disk space alert is based on the low watermark level. However, if you set the **Number of days in advance to trigger alert for low disk space for disk library** option to a value greater than 0, you receive a low disk space alert when the disk library is about to run out of space (measured in days). The warning message that you receive includes a failure reason. For example:

```
Failure Reason: At the current usage rate of 0.35GB per day, library <library name> with freespace 0.36GB will run out of space in 2 days.
```

To calculate the amount of space that remains, the system averages the amount of data that you backed up to the library over the last 30 days. In addition, the system subtracts the reserve space from the library’s free space so that the prediction is based only on the disk space that is available for jobs. Therefore, the calculation is: (disk space remaining – reserve space)/(average amount of data backed up over last 30 days) = # days when the library will be full.

For instructions, see Configuring a Low Disk Space Alert.

For more information about alerts, see Alerts and Monitoring.

CONFIGURE DISK VOLUME SIZE

Disk volumes are created based on the volume size. When the size of the volume reaches the maximum size, then a new volume is created. The maximum size of a disk volume is set to 100 GB by default, and this value can be modified. See Configure the Size of Disk Volumes for step-by-step instructions.

This operation is supported by all disk libraries.

CONFIGURE ARCHIVE FILES AS READ-ONLY

You can configure the library to create archive files as read-only files on filers. This feature can be enabled using the **Mark Archive Files as Read-Only** option in the Library Properties dialog box.

When this option is enabled, it engages the corresponding read-only lock mechanism on the destination filers and saves the archive/backup files as read-only files. The expiration date for the read-only lock is set to match the data retention time established in the storage policy copies. These archive files cannot be modified or deleted by any user or application until the specified retention date. Once the retention expires, the system deletes the archives as a part of Data Aging.

This feature is supported on the following filers:

- Data Domain (Archive Locks)
- EMC Celerra (File Level Retention)
- HDS HCP (Atime Retention)
- NetApp (SnapLock)
- Permabit (WORM Retention)
- HP StorageWorks X9000 6.0 Network Storage Systems

This option will only affect files that are subsequently created by data protection and auxiliary copy operations to this library. Permission to files that are already available in this library will not be affected.

See Create Read-Only Archive Files on filers for step-by-step instructions.

CONFIGURE TIMEOUTS

The timeout parameter determines how long a job waits for a status response after an operation is requested. If the job does not receive a success or failure status within the timeout period, the job is terminated and a failure message is displayed. You can set the following timeout periods:

- **MOUNT**

  The number of minutes used to mount the disk library for read/write operations.

- **UNMOUNT**

  The number of minutes used to unmount the disk library after a read/write operation.

See Modify the Mount and Unmount Timeouts for Disk Libraries for step-by-step instructions.

This operation is supported by all disk libraries.

ENABLE SUPPORT FOR SINGLE INSTANCING OF DATA (CONTENT ADDRESS STORAGE)

For appliances that support hardware single instancing of data (e.g., Centera) you can enable the option to write the data in a single instancing format.

See Enable Single Instancing of Data on a Disk Library for step-by-step instructions.

This feature requires a Feature License to be available in the CommServe® Server.

Review general license requirements included in License Administration. Also, View All Licenses provides step-by-step instructions on how to view the license information.

SUPPORT INFORMATION

The following Agents support this feature:

AGENT	**WHAT IS DEDUPLICATED**
Windows File System *i*DataAgent	Files (Meta-data associated with files are not deduplicated.)*****
Unix File System *i*DataAgents	Files
Macintosh File System *i*DataAgent	Files
NetWare File System *i*DataAgent	Files
Exchange Mailbox *i*DataAgent	Attachments
Exchange Mailbox Archiver	Attachments
Exchange Compliance Archiver	Attachments
SharePoint Document *i*DataAgent	Documents (Meta-data associated with documents are not deduplicated.)*****
File Archiver for Windows	Files (Meta-data associated with files are not deduplicated.)*****
File Archiver for Unix	Files

*****Metadata includes Access Control Lists (ACLs) and any additional streams associated with the files.

The following operations are not supported:

- Data Multiplexing to a deduplicated library.
- Auxiliary copy (including Inline Copy) of multiplexed data to a deduplicated library.

Once you have valid data in the library, you will not be able to change the deduplication status for the library, whether the option is enabled or not.

See Enable Single Instancing of Data on a Disk Library for step-by-step instructions.

ESTABLISH THE PARAMETERS FOR MOUNT PATH USAGE

These parameters may be used to specify how the system must perform write operations on disk libraries with multiple mount paths. Two parameters for mount path usage can be configured. They are:

- **FILL AND SPILL MOUNT PATHS**

  If this option is selected the system completely fills the disk space (based on the space allocation established for the individual mount paths) before writing to another mount path. Use this option when you want the data to be consolidated, without any fragmentation.

  The system will use the mount path in the order in which the mount path was added to the library. For example, a disk library has 3 mount paths (A, B, C) configured. All the jobs will be directed to mount path A as it was created first. Mount paths B and C will be used for additional writers in the order in which they were added to the disk library. Note that as long as a active volume exists in any of the mount paths, the consecutive backups will continue to use that mount path.

  SPILL AND FILL MOUNT PATHS

  If this option is selected the system writes to all the mount paths in parallel if you have established sufficient number of writers. Use this option to obtain maximum throughput , especially when you have several mount paths. However the data will be fragmented between the available mount paths.

  Note that when this option is selected, the system will use the Least Recently Used (LRU) mount path. (As opposed to the mount path with least used capacity.)

  For example, a disk library with 3 mount paths (A, B, C) and if two 3-stream storage policies (SP_1_1, 2 and 3 and SP_2_1, 2 and 3) are used for running simultaneous backups, the jobs are run as follows: (Assuming that the backups are run for the first time.)

  SP_1_1 > Mount Path A

  SP_2_1 > Mount Path B

  SP_1_2 > Mount Path C

  SP_2_2 > Mount Path A

  SP_1_3 > Mount Path B

  SP_2_3 > Mount Path C

  Note that this order may change subsequently, depending on the LRU condition of the mount path.

To illustrate the usage of the above mentioned options, consider the following example:

Assume that a disk library that allows multiple writes is configured with two mount paths. Start two jobs - the jobs may either be run concurrently, or individually, one after another. If the Fill and Spill mount paths option is selected, both jobs will use the first mount path. If the Spill and Fill mount paths option is selected, the first job will use the first mount path and the second will use the second mount path.

Note that data protection operations will continue with an available mount path if a required mount path is not available, thereby taking precedence over the option specified for mount path usage. For example, assume that that there are two mount paths, with the Spill and Fill mount path option selected. If one of the mount paths is not available, all data protection operations will use the available mount path.

See Establish the Mount Path Usage for a Disk Library for step-by-step instructions.

This operation is supported by all disk libraries.

THRESHOLDS FOR MANAGED DISK SPACE

Disks can be used to spool data prior to being permanently stored on tape for long term/offsite storage. Defining managed disk space thresholds allows you to retain your disk data longer by pruning data according to disk capacity and existing retention criteria.

You can define two-disk capacitcy thresholds for managed disk space:

- A threshold (in percentage) for starting the data aging operation (upper limit)
- A threshold (in percentage) for stopping the data aging (lower limit)

When disk capacity reaches a high threshold (e.g., 85%), any data exceeding its retention criteria is qualified for aging. When disk capacity reaches the low threshold (e.g., 70%),the aging process automatically stops.

Once the managed disk is set up the process runs automatically without user intervention to manage disk capacity. Data protection operations are retained on disk longer than usual providing the benefits of disk storage without having to spend manual efforts to manage the disk capacity.

The **Enable Managed Disk Space for disk data** option is available in the **Retention** tab of the **Copy Properties** dialog box. If a storage policy is created with a valid retention criteria other than infinite retention, then this option is automatically enabled in the copies.

The pre-defined thresholds for disk capacity for a disk library can be defined in the **Mount Paths** tab of the **Library Properties** (associated with a disk library) dialog box.

Data Aging determines the pruning based on jobs - jobs with older data (based on the creation time of its first archive file) is pruned first. Once the Data Aging operation determines the jobs to be pruned, data will be deleted based on the established threshold. The frequency for checking the disk space and deleting data is determined by the frequency established in the **Interval (Minutes) between disk space updates** option established in the **Service Configuration** tab of the **Media Management Configuration** dialog box in the **Control Panel**.

See Enable Managed Disk Space for Disk Data for step-by-step instructions.

See Data Aging for comprehensive information on data aging.

This operation is supported by all disk libraries.

ESTABLISH THE MOUNT PATH ALLOCATION POLICY FOR THE LIBRARY

The maximum number of writers for a disk library is used to determine the maximum number of simultaneous data protection operations. Hence this value is linked to the maximum number of data streams that can be established for a storage policy accessing the disk library.

Storage Policy data streams are logical channels that connect client data to the media in which data secured by data protection operations are stored. Multiple data streams can be used to parallelize an operation, in order to improve the rate at which data can be written to the media.

The practical limits for establishing data streams in a storage policy accessing a disk library is determined by the minimum value established in either the disk library or the sum of mount paths in the disk library.

The values for writers can be modified from the **Disk Library Properties** and **Mount Path Properties** dialog box available in the CommCell Console. The values for the maximum number of data streams can be modified from the **Storage Policy Properties** dialog box also available in the CommCell Console. See Establish the Mount Path Allocation Policy for a Disk Library for step-by-step instructions.

SEE ALSO:

- Writers and Storage Policy Data Streams
- Load Balancing between Disk Libraries

See Establish the Mount Path Allocation Policy for a Disk Library for step-by-step instructions.

This operation is supported by all disk libraries.

VIEW THE STORAGE POLICY AND STORAGE POLICY COPIES ACCESSING THE DISK LIBRARY

You can view the list of Storage Policies and the Storage Policy Copies accessing the disk library. See View a List of Storage Policies Accessing the Disk Library for step-step instructions.

This operation is supported by all disk libraries.

CONFIGURE SECURITY

Security allows you to associate the Disk library with one or more CommCell user groups. See User Administration and Security for a detailed explanation on user security.

This operation is supported by all disk libraries.

MIGRATE DISK LIBRARIES

You can migrate a disk library to another MediaAgent within the CommCell. Consider the following while performing this operation:

- To migrate a disk library, the target MediaAgent must have access to the same mount path as the source MediaAgent. Therefore, it is recommended that the target MediaAgent be created using mirroring. Mirroring allows one MediaAgent to be set up identically as another MediaAgent.
- If mirroring is not an option, the user must have mount paths that are accessible to the target MediaAgent. After migration, ensure that all mount paths are online or accessible.
- You can migrate a disk library if it was created in version 8.0 and the MediaAgent was upgraded to version 9.0, or if you created the disk library in version 9.0 with the EZ Operations Wizard.
- You cannot migrate a shared disk library.

See Migrate a Disk Library for step-by-step instructions.

FRAGMENTATION ANALYSIS

Fragmentation levels in the disk mount paths can be analyzed using the Fragmentation Analysis administrative job. When executed, the files in the selected mount paths are analyzed and the fragmentation statistics are reported in the Library and Drive Report. Based on the file fragmentation statistics reported, appropriate tools can be used to defragment the disk library.

> Bull Calypso recommends defragmenting disk library volumes when needed to ensure performance. Bull Calypso does not support calls on any Third-party defragmentation tools. However, Diskeeper has certified its 2011 (and higher) release version for online volume defragmentation.

Before using this feature, set the desired fragmentation margin using the following two parameters in the Media Management Configuration (Service Configuration) tab:

- **Per File Fragmentation Threshold** - Specify the number of fragments per file fragmentation limit per file, beyond which the file is considered fragmented. Default value is set to 10.
- **Mount Path Fragmentation Threshold Percentage** - Specify the fragmentation threshold percentage for the mount path. If the threshold exceeds this percentage, then the Library Management Maintenance Required alert, if configured, will be triggered. Default value is set at 100. See Alerts - Media Management for details.

See Perform Fragmentation Analysis for step-by-step instructions. The results of the job can be viewed from the Disk library Maintenance Job Summary Report.

This feature is supported on Windows MediaAgents. Note that this feature is not supported on Centera Clusters.

Fragmentation levels in the mount path can be reduced by using configuration options. See Reduce Fragmentation of Data on a Mount Path for more information.

HOW IS DISK FRAGMENTATION CALCULATED FOR DISK LIBRARIES?

For all files in a mount path, Bull Calypso utilizes the following formula to determine the fragmentation percentage:

(Total number of excess fragmentation/Total number of allowed fragmentation) * 100

The **Per File Fragmentation Threshold** configuration parameter available in Media Management Configuration (Service Configuration) tab sets the number of allowed fragments per file. The default value is 10. This means within the 2GB chunks of a mount path, if the number of fragments is above 10 (suppose n, where n>10), then the file is categorized as a fragment and the excess fragment (n-10) is counted.

The following is an example of a mount path with five chunks (assuming a block size of 4096K as block content, below a value of 4096 will have no fragments).

Per-file fragmentation threshold = 10

Name (files)	Size	Number of Fragments	Number of Excess Fragments
MEDIA_LABEL	64K	0	0
CHUNK_1	2GB	53	43
CHUNK_2	2GB	9	0
CHUNK_3	2GB	14	4
CHUNK_4	2GB	26	16
CHUNK_5	2GB	5	0
CMT_1	64K	0	0
CMT_2	64K	0	0
CMT_3	64K	0	0
CMT_4	64K	0	0
CMT_5	64K	0	0

The mount path in the above table shows excess fragmentation = 63 (43 + 4 + 16)

Total number of files = 11

Allowed fragmentation = (total number of files * per-file fragmentation threshold) = 11 * 10 = 110

Total fragmentation percentage = (Total excess fragmentation / Total allowed fragmentation) * 100

= (63 * 110) * 100 = 63%

> You can increase/decrease per-file fragmentation threshold to control the fragmentation percentage watermark.

DISK VOLUME RECONCILIATION

Disk volume reconciliation allows you to reconcile the discrepancies in the disk volume associated with a storage policy copy data. This feature compares the physical data located in the disk mount path with the metadata records in the CommServe database and provides the list of orphaned jobs and orphaned media space. Orphaned jobs are jobs without corresponding data on the media, and orphaned media is the list of volumes without corresponding jobs in the CommServe. This feature is applicable for disk storage media only.

The orphaned media is displayed with associated details like the Storage Policy, Storage Policy Copy, Library, volume path, No. of Chunks, Size of the data etc., and the orphaned jobs are displayed with details such as Job ID, Client Name, Application Type, Library, Storage Policy, Storage Policy Copy, etc. You can review the information and delete the orphaned jobs and/or orphaned media. When an orphaned media space is deleted, the space is marked for deletion and pruned based on the retention rules set for the copy. When an orphaned job is deleted, the job is removed from the CommServe database. Jobs deleted using this feature are recorded in the Audit Trial. See Perform a Disk Volume Reconciliation Job and Reconcile the Differences for step-by-step instructions.

Once a disk volume reconciliation job is executed, you can use the results of the analysis to reconcile the differences at a later time. This allows you to reconcile the differences without executing the job again. See View the Results of a Disk Volume Reconciliation Job and Reconcile the Differences for step-by-step instructions.

> This feature is supported only for Non-Deduplicated Storage Policy copy.

You can use the Media Information Report to review the results of this job. The details of the orphaned jobs, orphaned media, and the volumes deleted using the job are available in the report.

ADMINISTERING MOUNT PATHS

From the CommCell Browser, you can perform the following operations on a mount path:

VIEW OR MODIFY THE PROPERTIES OF THE MOUNT PATH

You can view the mount path location and information on the free space available on the mount path and the total amount of valid data. If necessary you can record pertinent information about the mount path as a description in the mount path properties.

This operation is supported by all disk libraries.

USE UNBUFFERED I/O

To increase the speed of operations accessing the mount path, you can enable the MediaAgent to bypass the Microsoft Windows file system buffering. Note that this option is only applicable for Windows MediaAgents and disks that are directly mounted (not UNC paths. (See Enable Unbuffered I/O on a Mount Path or step-by step instructions on enabling this option.)

Note that this is a licensed feature and requires a feature license to be available on the CommServe.

See Enable Unbuffered I/O on a Mount Path for step-by-step instructions.

ENABLE OR DISABLE A MOUNT PATH

The mount path can be enabled or disabled, if required, to control the access to the mount path. If the mount path is disabled, it will be displayed as *Offline* in the **General** tab of the **Mount Path Properties** dialog box. If the mount path is disabled by the system due to inaccessibility, the offline reason can also viewed from the **General** tab of the **Mount Path Properties** dialog box. Note that when a MediaAgent itself is offline, the individual mount paths are not displayed as offline.

See Enable or Disable a Mount Path for step-by-step instructions.

This operation is supported by all disk libraries.

ESTABLISH THE MOUNT PATH ALLOCATION POLICY

The mount path allocation policy allows you to establish the maximum number of concurrent writers or the maximum number of simultaneous data protection operations on the mount path. See Establish the Mount Path Allocation Policy for the Library for a detailed description.

If necessary you can also disable the mount path for write operation. This is useful in situations where you wish to retire or phase-out a mount path. See Retire a Mount Path for step-by-step instructions.

This operation is supported by all disk libraries.

ESTABLISH SPACE ALLOCATION ON THE MOUNT PATH

Space allocation allows you to establish the maximum amount of space that must be used by the mount path. This can be done by specifying the reserve space and selecting either the **Use until the mount path reaches the reserved space** or **Do not consume more than n GB** options.

> The **Do not consume more than n GB** option considers the backup size stored in the mount path. That is, the data size after compression and before deduplication.

- In some situations the mount path may consume more space and exceed the specified minimum reserve space. Consider the following example:

  If you have established the minimum reserve space as 2 GB, and run a 2 streamed data protection operation when the disk space is 2.01 GB, both the streams will use a minimum of 25 MB before spanning to an alternate mount path. In such a situation the free space will fall below the specified 2 GB.

  This could also happen if 2 concurrent single-streamed data protection operation is initiated to the same mount path, using 2 different storage policies.

- Similarly, the system may consume more than the specified maximum space. Consider the following example:

  When a data protection job is initiated, the system checks for the available disk space and verifies whether it is less than the specified maximum space. For example if you have specified 5 GB as the maximum space and if you have used 4.75 GB, the data protection job will be initiated using the mount path. However, if the size of the data is .5 GB, the system will write the entire data. In such a situation the space consumed will be more than the specified maximum space.

Note that a data protection operation will generally write to the mount path until the minimum reserve space is reached, before spanning to an alternate path.

See Establish Maximum Space Allocation on a Mount Path for step-by-step instructions.

This operation is supported by all disk libraries.

REDUCE FRAGMENTATION OF DATA ON A MOUNT PATH

You can reduce the fragmentation of data on a mount path by enabling the **Reduce fragmentation by growing the backup chunk by n MB** option. This will pre-allocate the space on the mount path for a write operations resulting in reduced fragmentation which in turn will speed-up read operations (auxiliary copy, restore operations) from the disk. This option is supported only for Windows MediaAgents. See Reduce Data Fragmentation on a Mount Path for step-by-step instructions.

Note that fragmentation levels in the mount path can be analyzed using the Fragmentation Analysis feature.

VIEW THE CONTENTS OF A MOUNT PATH

You can view the contents of a specific mount path. This feature can be used to view a list of data protection operations residing in the mount path. All the details associated with the data protection operation(s) available in the media are displayed. This includes the following:

- The Job ID and the status associated with the data protection operation
- Names of the client, agent, instance/backup set and subclient
- Whether the data protection operation is Full, Incremental, Differential or Synthetic full
- The archive file type
- The day and time in which the archive file associated with the data protection operation was created.

See View the Contents of a Mount Path for step-by-step instructions.

This operation is supported by all disk libraries.

DELETE THE CONTENTS OF A MOUNT PATH

The delete contents option can be used to logically delete the contents of a mount path.

This operation deletes the data from the CommServe database. Note that this operation does not free-up the disk space in the mount path. A Data Aging operation must be run subsequently to free-up the disk space.

This option can be used to make media available to complete an important data protection job when there is no free-space available in the library.

CAUTION

Extreme caution should be exercised while using this option as once deleted, the contents of the mount path will not be available for data recovery operations.

The Delete Contents operation is recorded in the Audit Trail.

See Delete the Contents of a Mount Path for step-by-step instructions.

This operation is supported by all disk libraries.

PREVENT ACCIDENTALLY DELETING THE CONTENTS OF A MOUNT PATH

You can protect your mount path contents from being accidentally deleted outside of the CommCell Console. Contents on mount paths created when this feature is enabled are protected from accidental deletion. See Prevent Accidentally Deleting Mount Path Contents for step-by-step instructions to enable/disable this feature. This feature is enabled by default.

This feature applies to mount paths created on NTFS volumes. This feature is not supported on libraries attached to BlueArc NAS NDMP file servers, Hitachi HNAS storage array and Data Domain storage systems.

MOVING MOUNT PATHS

There are two ways to move the mount paths to another location:

- Move the contents of the entire mount path to another location. See Move a Mount Path for step-by-step instructions.
- Retire (phase out) or move subsequent operations to another location and allow the data in the current location to be aged by the data aging operation. See Retire a Mount Path. for step-by-step instructions.

You can also attach the disk library to another MediaAgent by migrating a disk library. See Migrate a Disk Library for step-by-step instructions.

VIEW OR MODIFY THE PROPERTIES OF SHARED DISK DEVICES FOR STATIC MOUNT PATHS

You can view or modify the device alias name and can enable or disable the device. See View or Modify the Device Properties for Disk Libraries with Static Mount Paths for step-by step instructions.

VIEW OR MODIFY THE DEVICE PATHS ASSOCIATED WITH SHARED DISK DEVICES

You can also view and modify the following properties associated with device paths associated with shared disk devices from a mount path:

- List of device paths and their associated MediaAgents accessing the shared device
- The path used to access the device
- The username used to access the device
- The access permissions for the device
- View or modify the maximum number of writers to the device
- Enable or disable the MediaAgent's access to the device

See View or Modify the Properties of Disk Devices in a Shared Mount Path for step-by-step instructions.

This operation is supported by all shared disk libraries, which includes disk libraries on static shares and replicated disks.

MODIFY THE READ/WRITE ACCESS TO A MOUNT PATH IN REPLICATED DISKS

See View or Modify the Properties of Disk Devices in a Shared Mount Path for step-by-step instructions.

AUDIT TRAIL

Operations performed with this feature are recorded in the Audit Trail. See Audit Trail for more information.

LICENSE REQUIREMENTS

This feature requires a Feature License to be available in the CommServe® Server.

Review general license requirements included in License Administration. Also, View All Licenses provides step-by-step instructions on how to view the license information.

OTHER CONSIDERATIONS

- The CV_MAGNETIC folder (which is created when a mount path is configured) will by default be excluded from data protection operations if a MediaAgent and the Windows File System *i*DataAgent is installed in a computer. (The CV_MAGNETIC folder must be associated with the MediaAgent that is installed in the computer.) To include the folder in data protection operations, the nDoNotFilterGalaxyMagneticMountPaths registry key must be created in the computer.
- By default the system uses 2 GB as the chunk size and 64K as the block size to read/write data from disk libraries. If necessary, these values can be modified per data path, from the **Data Path Properties** dialog box available from the **Data Paths** tab of the **Copy Properties** dialog box, for the specific data path. (See Set the Chunk Size and Block Size for a Data Path for step-by-step instructions.)

  For more information on using chunk and block sizes, see Performance Tunables for Media Management.

RELATED ALERTS

The following Media Management Library Management alerts can be configured from the Alerts Wizard:

- Insufficient Storage
- Maintenance Occurred
- Maintenance Required
- Media Handling Required
- Media Mount and Usage Errors
- User Overwrite of Media
- Media Ready in Mail Slot
- Media Recalled

For more information, see:

- Alerts: Media Management
- Configure Alerts

Back to Top

Disk Libraries - Configure

Topics | Configure | How To | Troubleshoot | Related Topics

CONFIGURE A DISK LIBRARY

The following procedure describes the steps involved in configuring a disk library.

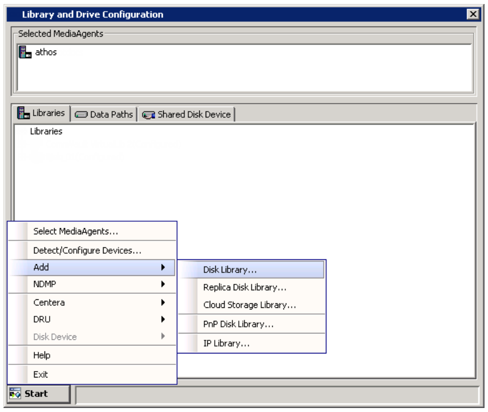
BEFORE YOU BEGIN

This feature requires a Feature License to be available in the CommServe® Server.

Review general license requirements included in License Administration. Also, View All Licenses provides step-by-step instructions on how to view the license information.

TO CONFIGURE A DISK LIBRARY

1. Display the Library and Drive Configuration window.
2. From the **Library and Drive Configuration** window, click the **Start** menu, select **Add**, then select **Disk Library** from the shortcut menu.

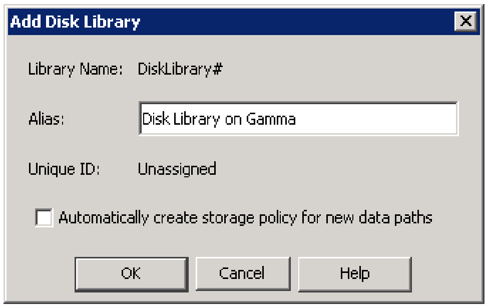


3. In the **Add Disk Library** dialog box, add the following information:

   Alias: A descriptive name for the disk library.

   Automatically create storage policy for new data paths: Select this option to automatically create a new storage policy when the mount path is added to this disk library.

   Click **OK**.


Add Disk Library

Library Name: DiskLibrary#

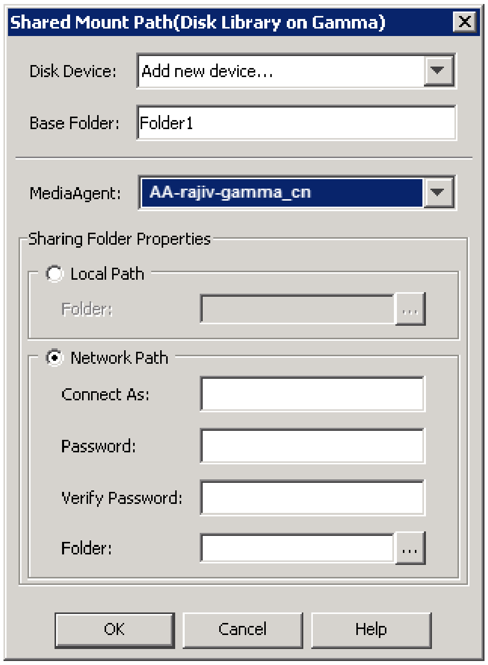
Alias: Disk Library on Gamma

Unique ID: Unassigned

☐ Automatically create storage policy for new data paths

4. In the **Add Mount Path** dialog box, select either **Local Path** or **Network Path**.
   - Choose the **Add new device..** option from the **Disk Device** list.
   - If necessary add a name of the folder in which the library must be created in the **Base Folder** box.
   - Choose the name of the associated **MediaAgent**.
   - If you select **Local Path**, click **Browse** to select a mount path, or enter a mount path.
   - If you select **Network Path**, type the user name and password to access the network share. Click **Browse** to select a mount path, or enter a mount path.

     For Unix MediaAgent, you can choose only a local path. To access NFS share, you must mount the share to your Unix MediaAgent. Once mounted, the share appears as another local directory on the system and then you can provide this directory location in the local path.
   - Click **OK**.


Shared Mount Path(Disk Library on Gamma)

Disk Device: Add new device...

Base Folder: Folder1

MediaAgent: AA-rajiv-gamma_cn

Sharing Folder Properties

○ Local Path

Folder:

● Network Path

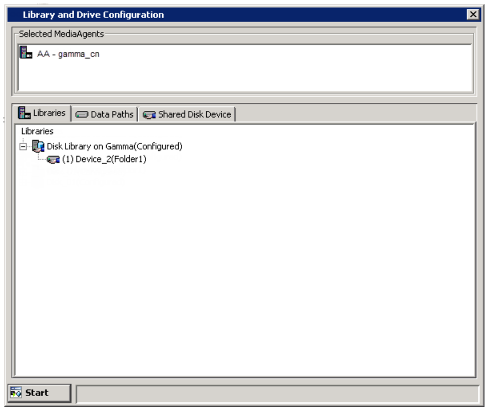
Connect As:

Password:

Verify Password:

Folder:

The mount path is added to the specified location. When you add a mount path, the disk library appears in the **Library and Drive Configuration** window with a status of configured.


Library and Drive Configuration

Selected MediaAgents

AA - gamma_cn

Libraries | Data Paths | Shared Disk Device

Libraries

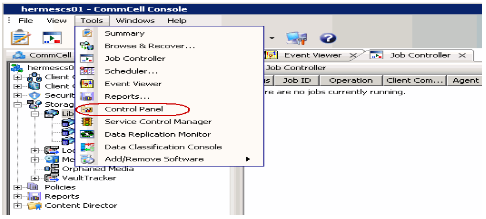
Disk Library on Gamma(Configured)

(1) Device_2(Folder1)

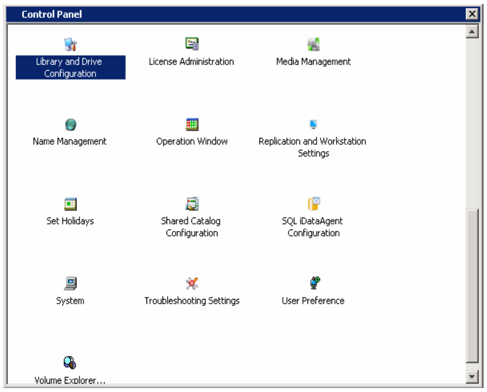
Configuring Automatic Mount Paths for New Disk Storage

The following procedure described the steps involved in configuring automated disk library.

1. From the CommCell Console, click the Tools menu and then click **Control Panel**.

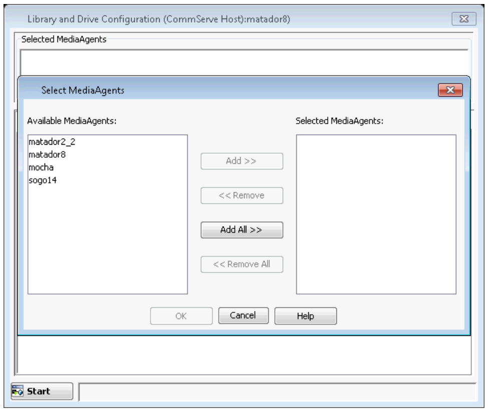


2. From the Control Panel, double-click the **Library and Drive Configuration**.

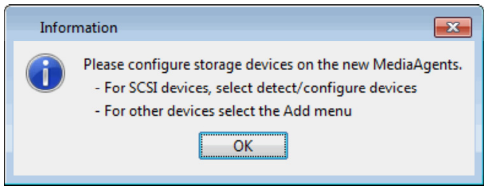


3.

- Select the MediaAgent(s) whose devices you want to detect or display from the **Available MediaAgents** list box.
- Click **Add >>** to move the MediaAgent(s) to the **Selected MediaAgents** list box.
- Click **OK**.

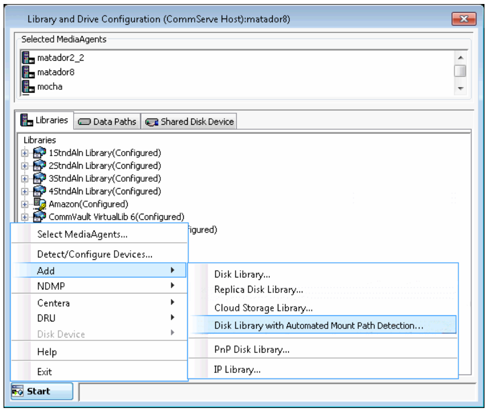


4. Click **OK**.

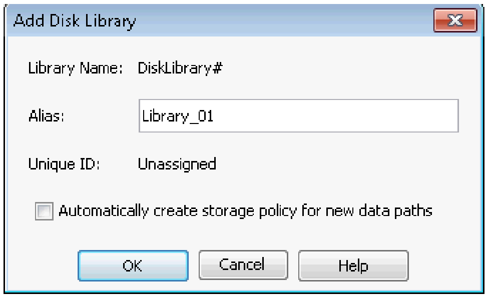

Information

Please configure storage devices on the new MediaAgents.
- For SCSI devices, select detect/configure devices
- For other devices select the Add menu

5. From the **Library and Drive Configuration** window, click the **Start** menu, select **Add**, and then click **Disk Library with Automated Mount Path Detection...**


Library and Drive Configuration (CommServe Host):matador8)
Selected MediaAgents
matador2_2
matador8
mocha
Libraries
Data Paths
Shared Disk Device
Libraries
1StndAln Library(Configured)
2StndAln Library(Configured)
3StndAln Library(Configured)
4StndAln Library(Configured)
Amazon(Configured)
CommVault VirtualLib 6(Configured)
figured)
Select MediaAgents...
Detect/Configure Devices...
Add
NDMP
Centera
DRU
Disk Device
Help
Exit
Disk Library...
Replica Disk Library...
Cloud Storage Library...
Disk Library with Automated Mount Path Detection...
PnP Disk Library...
IP Library...
Start

6. In the **Alias** box, specify name of the disk library and then click **OK**.


Add Disk Library

Library Name: DiskLibrary#

Alias: Library_01

Unique ID: Unassigned

☐ Automatically create storage policy for new data paths

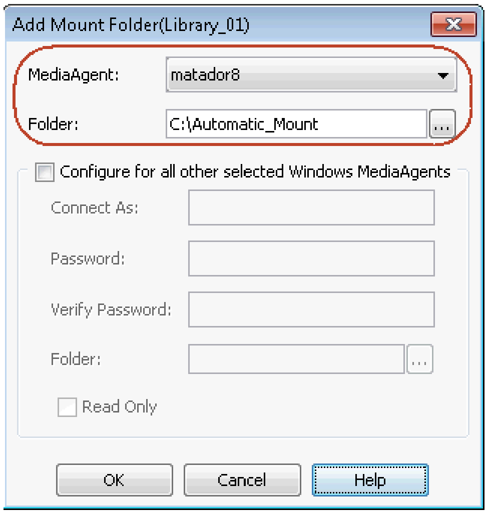
7.

- From the **MediaAgent** list, select the MediaAgent.

- In the **Folder** box, type the mount path or click **Browse [...]** to select a mount path.

  If you need to share the volumes across MediaAgents, share the mount folder. This will automatically share the newly added volumes.

- Click **OK**.



Add Mount Folder(Library_01)

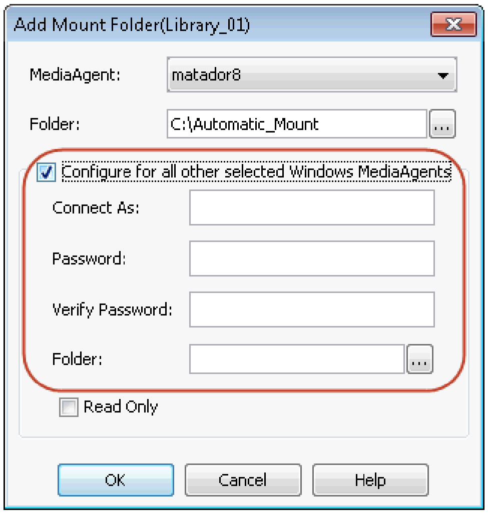
MediaAgent: matador8

Folder: C:\Automatic_Mount

8. If you wish to configure mount path for all selected MediaAgent(s), perform the following:

   - Select **Configure for all other selected Windows MediaAgents** check box.
   - In the **Connect As** box, specify the user account information.
   - In the **Password** box, specify the password to access the mount path.
   - In the **Verify** Password, re-type the password.
   - In the **Folder** box, type the mount path or click **Browse [...]** button to select a mount path.
   - Select **Read Only** check box, to give read only permission to the mount path.
   - Click **OK**.

   The libraries will be shared between all MediaAgents as per the mount folder specified at the time of configuration.



Add Mount Folder(Library_01)

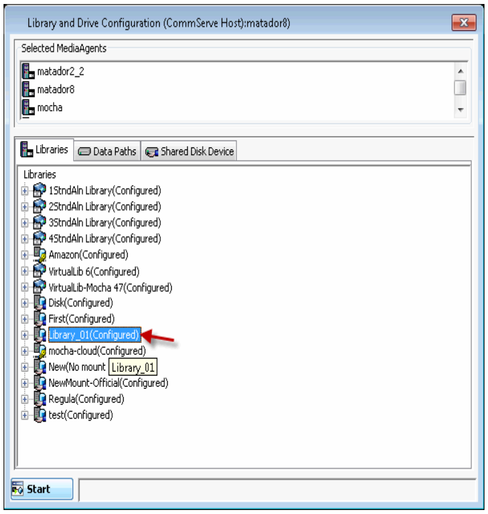
MediaAgent: matador8

Folder: C:\Automatic_Mount

☑ Configure for all other selected Windows MediaAgents

9. The mount path is added to the specified location. When you add a mount path, the disk library appears in the **Library and Drive Configuration** window with a status of configured.

   If a MediaAgent is removed from the mount folder device list, it will not affect the libraries already configured.



Library and Drive Configuration (CommServe Host):matador8)

Selected MediaAgents

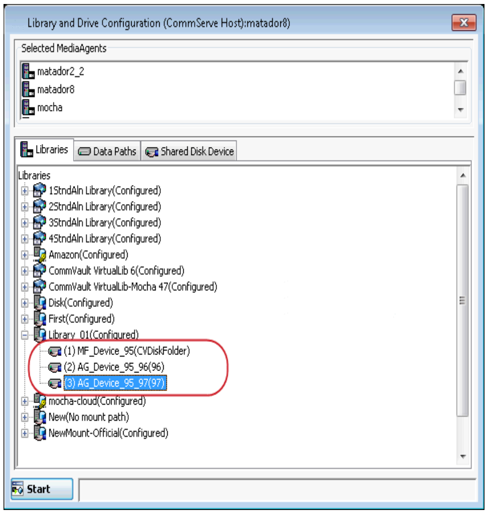
- matador2_2
- matador8
- mocha

Libraries

- 1StndAln Library(Configured)
- 2StndAln Library(Configured)
- 3StndAln Library(Configured)
- 4StndAln Library(Configured)
- Amazon(Configured)
- VirtualLib 6(Configured)
- VirtualLib-Mocha 47(Configured)
- Disk(Configured)
- First(Configured)
- Library_01(Configured)
- mocha-cloud(Configured)
- New(No mount Library_01
- NewMount-Official(Configured)
- Regula(Configured)
- test(Configured)

10. Expand library to see the devices added to the mount path.

    When a new LUN is mounted under the mount folder as a mount point, the LUN will be automatically detected during next magnetic space check and will create a new Device.

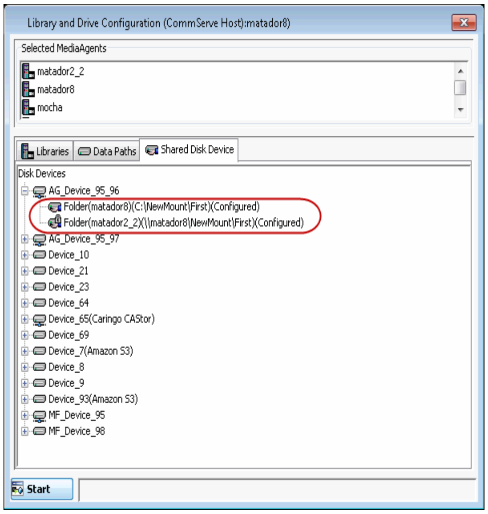

Library and Drive Configuration (CommServe Host):matador8)
Selected MediaAgents
matador2_2
matador8
mocha
Libraries
Data Paths
Shared Disk Device
Libraries
1StndAln Library(Configured)
2StndAln Library(Configured)
3StndAln Library(Configured)
4StndAln Library(Configured)
Amazon(Configured)
CommVault VirtualLib 6(Configured)
CommVault VirtualLib-Mocha 47(Configured)
Disk(Configured)
First(Configured)
Library_01(Configured)
(1) MF_Device_95(CVDiskFolder)
(2) AG_Device_95_96(96)
(3) AG_Device_95_97(97)
mocha-cloud(Configured)
New(No mount path)
NewMount-Official(Configured)
Start

11. If you have configured multiple MediaAgent for the mount path as described in step 8, then perform the following to see the MediaAgents that are shared for the mount paths:

- Click **Shared Disk Device** tab.
- Expand the ***<Device>***.

The MediaAgent(s) configured with the device will be displayed.

If you have configured MediaAgent with read only permission, a lock 🔒 icon will appear at the mount path.



12. Also, you can set this **Automatic mount path detection** configuration for existing library. See Add Automatic Mount Path Detection for step-by-step instructions.

CONFIGURE SHARED DISK LIBRARIES WITH STATIC MOUNT PATHS

The following procedure describes the steps involved in configuring a shared disk library with static mount paths.

BEFORE YOU BEGIN

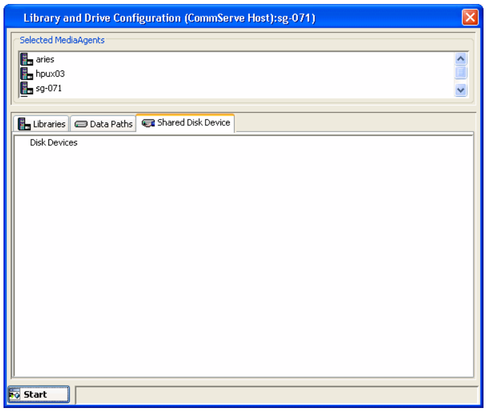
This feature requires a Feature License to be available in the CommServe® Server.

Review general license requirements included in License Administration. Also, View All Licenses provides step-by-step instructions on how to view the license information.

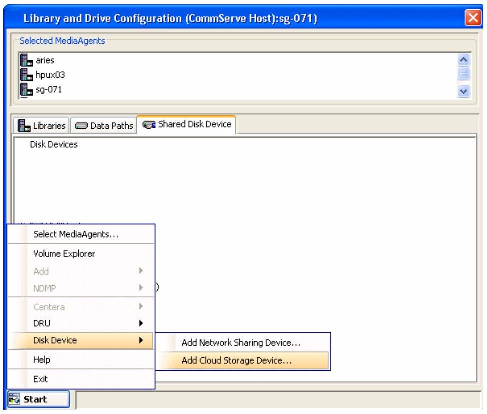
TO CONFIGURE A SHARED DISK LIBRARY WITH STATIC MOUNT PATHS

1. Display the Library and Drive Configuration window.

2. Click the **Shared Disk Device** tab.



3. Click the **Start** menu, select **Disk Device**, then choose **Add Network Sharing Device**.

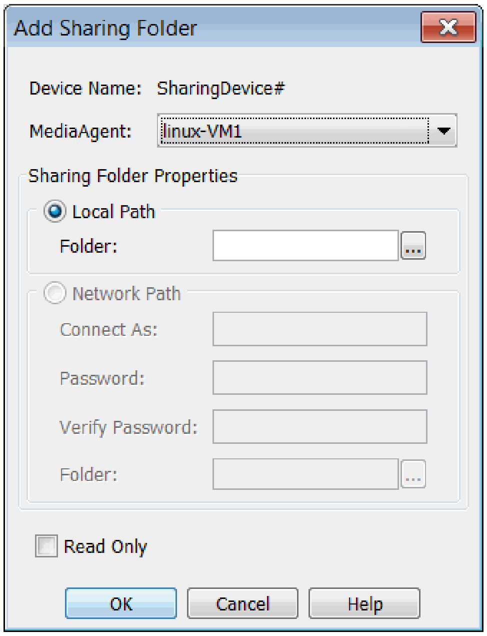


4. In the **Add Sharing Folder** dialog box, enter/select the following information:
   - **MediaAgent** - The name of the MediaAgent accessing the mount path.
   - **Folder** - The network path that will be used by the MediaAgent to access the mount path

     If the MediaAgent is a Windows MediaAgent, you can choose a local path or a network path. If you use a network path provide the username and password that must be used by the system to access the device.

     If the MediaAgent is a Unix/Linux MediaAgent, then you can choose only a local path. To access NFS share, you must mount the share to your Unix/Linux MediaAgent. Once mounted, the share appears as another local directory on the system and then you can provide this directory location in the local path.
   - When you are finished, click **OK**.

     When configuring a PolyServe File System, use the local PolyServe exposed volume instead of using UNC paths as the folder.



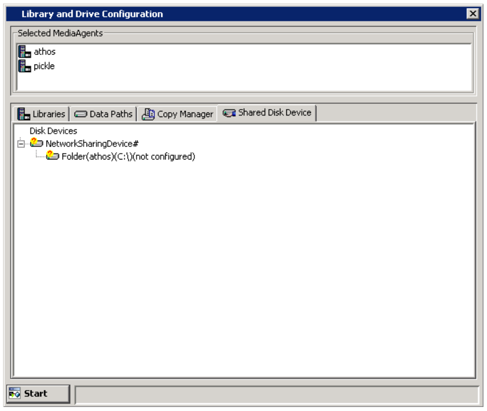
Device Name: SharingDevice#

MediaAgent: linux-VM1

● Local Path

Folder:

5. The system displays the device information with the MediaAgent accessing the device in the **Library and Drive Configuration** window.



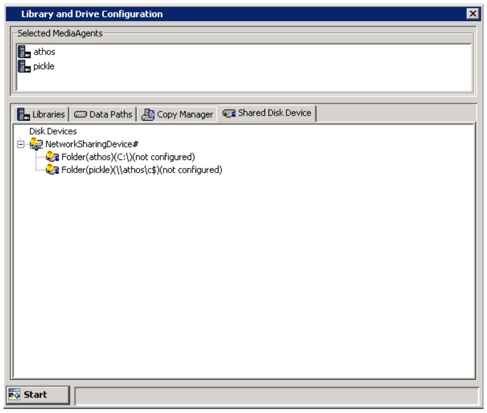
athos
pickle

Disk Devices
NetworkSharingDevice#
Folder(athos)(C:\)(not configured)

6. If you would like to add another MediaAgent to access the device, right-click the appropriate **NetworkSharingDevice** and then click **Add Primary Sharing Folder**.

   Enter/select the necessary information in the **Add Sharing Folder** dialog box, as described in Step 4.

   Repeat this step to add all the mount paths to the device.



athos
pickle

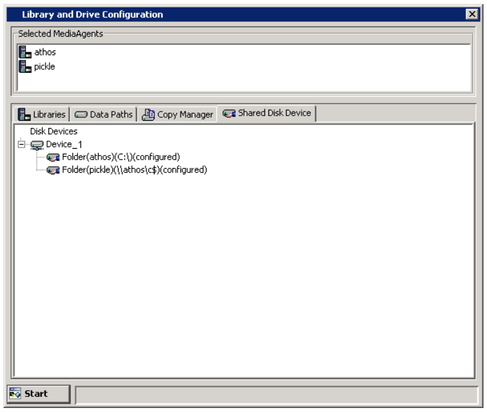
Disk Devices
NetworkSharingDevice#
Folder(athos)(C:\)(not configured)
Folder(pickle)(\\athos\c$)(not configured)

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

7. Right-click the **Network Sharing Device** and then click **Configure**.

8. Click **Yes** in the **Confirm Configure** prompt.

   The status of the folders changes to **configured**.

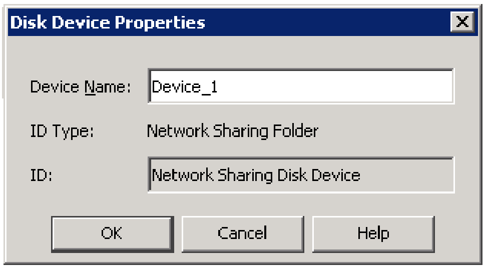


athos
pickle

Disk Devices
Device_1
Folder(athos)(C:\)(configured)
Folder(pickle)(\\athos\c$)(configured)

9. Optionally rename the Device Name with an appropriate name, to avoid confusion.

   To rename, right-click the device and then click **Properties**. In the **Device Properties** dialog box, type a new name.



Device Name: Device_1

ID Type: Network Sharing Folder

ID: Network Sharing Disk Device

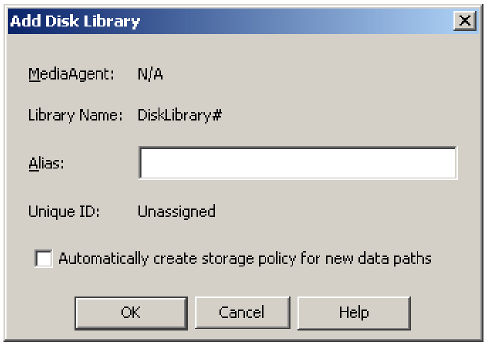
10. From the **General** tab of the **Library and Drive Configuration** window, click the **Start** menu, select **Add**, then choose **Disk Library**.

11. In the **Add Disk Library** dialog box, enter the following:

    Alias: A descriptive name for the disk library.

    Automatically create storage policy for new data paths: Select this option to automatically create a new storage policy when the mount path is added to this disk library.

Click **OK**.



Add Disk Library

MediaAgent: N/A

Library Name: DiskLibrary#

Alias:

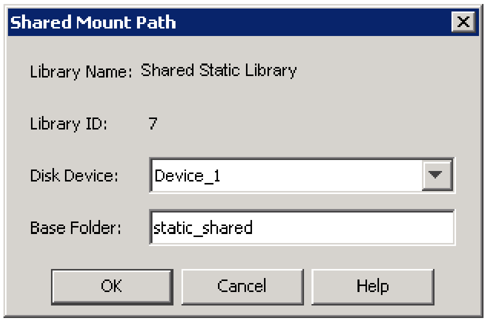
Unique ID: Unassigned

☐ Automatically create storage policy for new data paths

12. In the **Shared Mount Path** dialog box, select the disk device that you wish to associate as the mount path from the **Disk Device** list.

    In the **Base Folder** box, type the name of the base folder under which the mount path can store data. Do not include the drive letter while adding the name of the base folder.

    Click **OK**.



Shared Mount Path

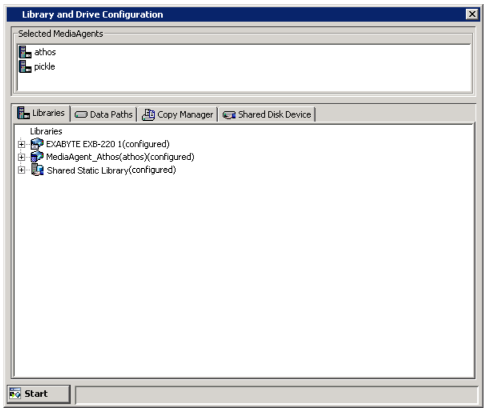
Library Name: Shared Static Library

Library ID: 7

Disk Device: Device_1

Base Folder: static_shared

The mount path is added to the shared disk library.



Library and Drive Configuration

Selected MediaAgents

athos

pickle

Libraries

EXABYTE EXB-220 1(configured)

MediaAgent_Athos(athos)(configured)

Shared Static Library(configured)

CONFIGURE DISK LIBRARIES ON REPLICATED DISKS

The following procedure describes the steps involved in configuring a shared disk library with static mount paths.

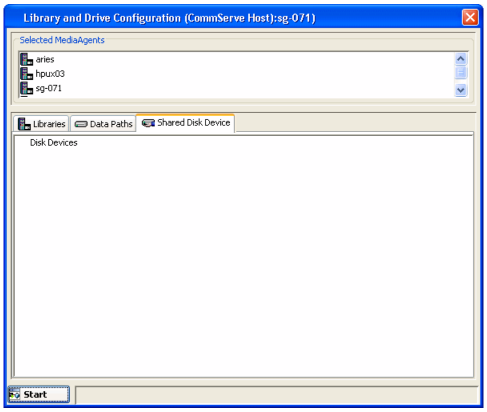
BEFORE YOU BEGIN

This feature requires a Feature License to be available in the CommServe® Server.

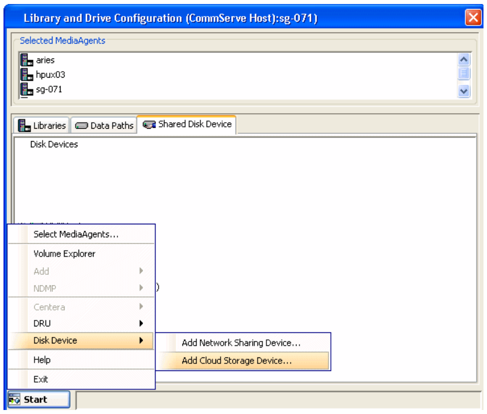
Review general license requirements included in License Administration. Also, View All Licenses provides step-by-step instructions on how to view the license information.

TO CONFIGURE DISK LIBRARIES ON REPLICATED DISKS

1. Display the Library and Drive Configuration window.
2. Click the **Shared Disk Device** tab.



3. Click the **Start** menu, select **Disk Device**, then choose **Add Network Sharing Device**.



4. In the **Add Sharing Folder** dialog box, enter/select the following information:

MediaAgent - The name of the MediaAgent accessing the mount path.

Folder - The network path that will be used by the MediaAgent to access the mount path

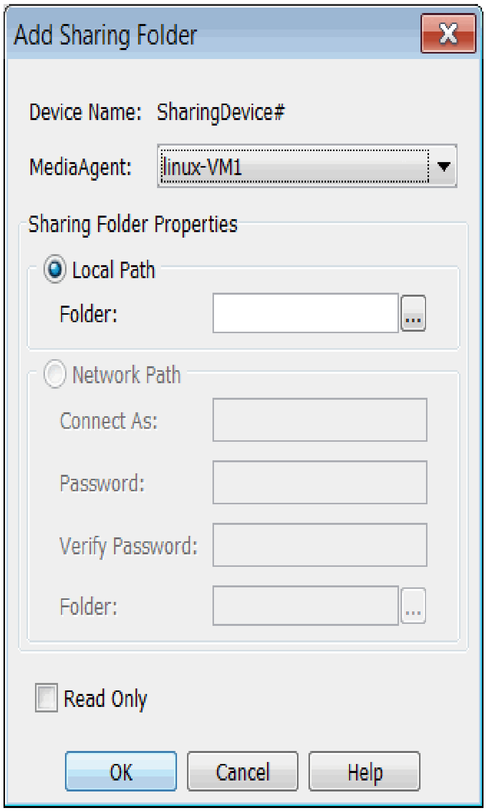
If the MediaAgent is a Windows MediaAgent, you can choose a local path or a network path. If you use a network path provide the username and password that must be used by the system to access the device.

NOTES:

- Network path is not supported for Disk Library Replication solution; only local paths are supported.

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

Click **No** in the confirmation dialog box to add another sharing folder.



Device Name: SharingDevice#

MediaAgent: linux-VM1

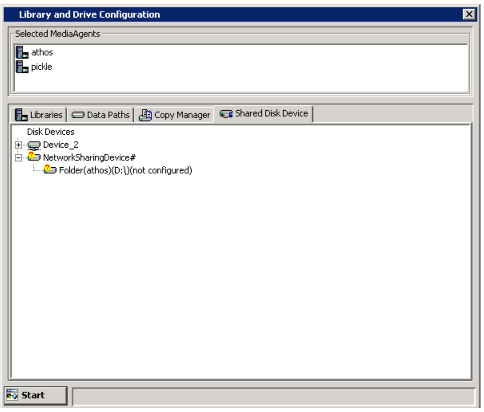
● Local Path

Folder:

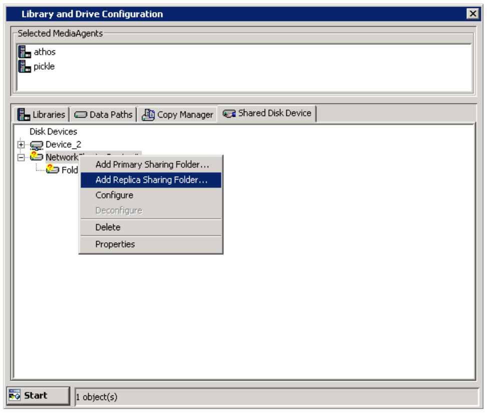
○ Network Path

□ Read Only

The system displays the device information with the MediaAgent accessing the device in the **Library and Drive Configuration** window.



5. Right-click **NetworkSharingDevice** and then click **Add Replica Sharing Folder**.



6. In the **Add Sharing Folder** dialog box, enter/select the following information for the MediaAgent residing on the replica sharing folder.

   MediaAgent - The name of the MediaAgent accessing the mount path.

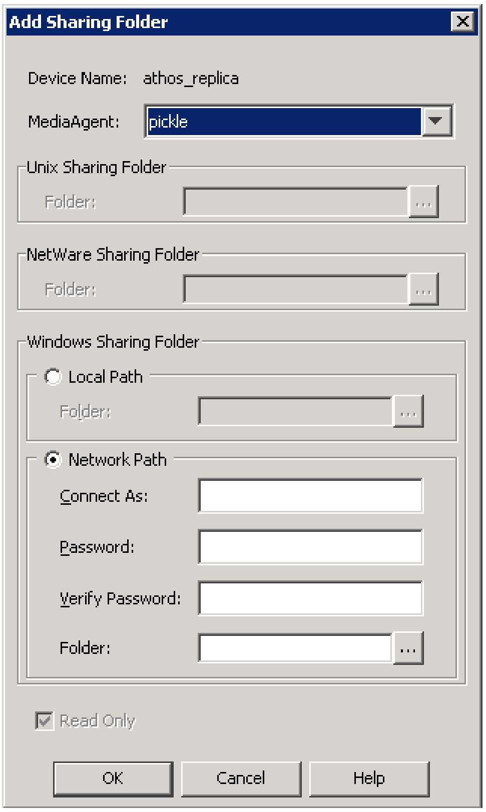
   Folder - The path that will be used by the MediaAgent to access the mount path

   If the MediaAgent is a Windows MediaAgent, you can choose a local path or a network path. If you use a network path provide the username and password that must be used by the system to access the device.

   NOTES:

   - Network path is not supported for Disk Library Replication solution; only local paths are supported.
   - For Disk Library Replication solution, this is the destination sharing folder and cannot be the same as the sharing folder path given in Step 4.

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


Add Sharing Folder

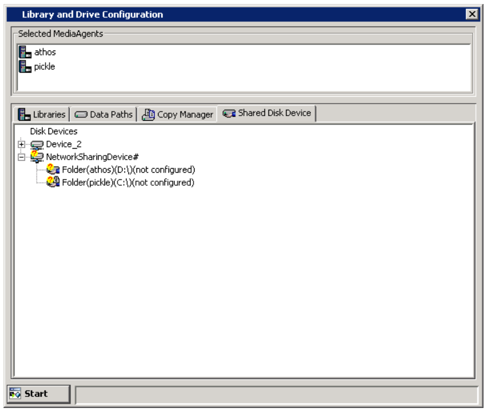
Device Name: athos_replica

MediaAgent: pickle

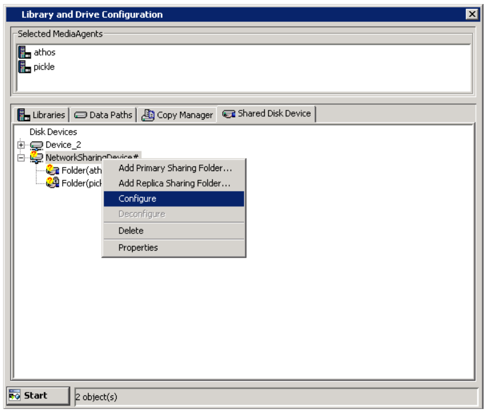
Windows Sharing Folder: ● Network Path

☑ Read Only

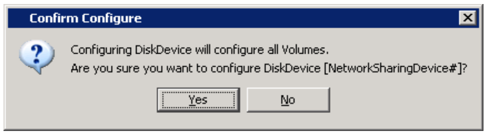
The system displays the device information with the MediaAgent accessing the device in the **Library and Drive Configuration** window.



7. Right-click **NetworkSharingDevice** and then click **Configure**.

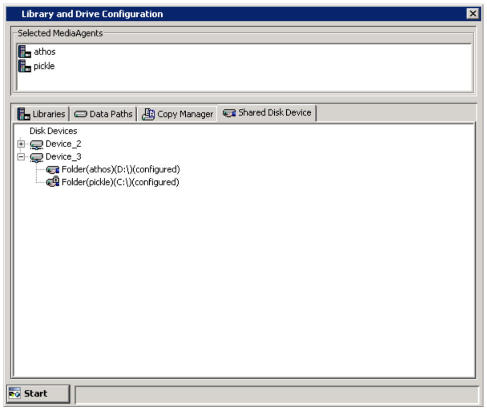


8. Click **Yes** to continue.



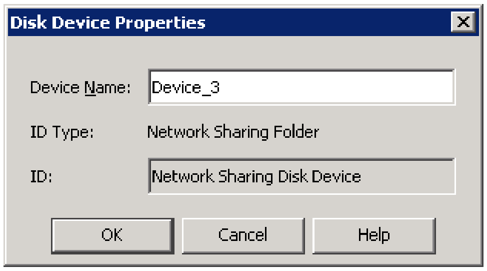
Configuring DiskDevice will configure all Volumes.
Are you sure you want to configure DiskDevice [NetworkSharingDevice#]?

The status of the folders changes to **configured** in the **Library and Drive Configuration** window.



9. Optionally rename the Device Name with an appropriate name, to avoid confusion.

   To rename, right-click the device and then click **Properties**. In the **Device Properties** dialog box, type a new name.

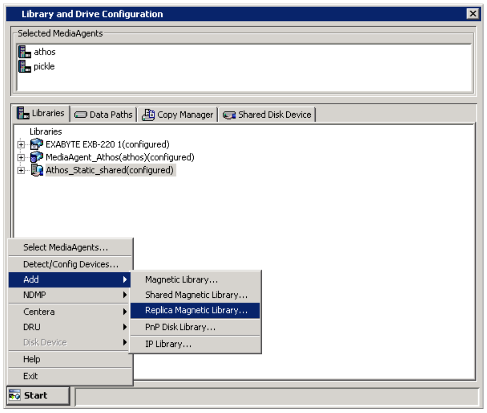


Device Name: Device_3

ID Type: Network Sharing Folder

ID: Network Sharing Disk Device

10. From the **General** tab of the **Library and Drive Configuration** window, click the **Start** menu, select **Add**, then choose **Replica Disk Library**.



11. In the **Add Disk Library** dialog box, enter the following:

Alias: A descriptive name for the disk library.

Automatically create storage policy for new data paths: Select this option to automatically create a new storage policy when the mount path is added to this disk library.

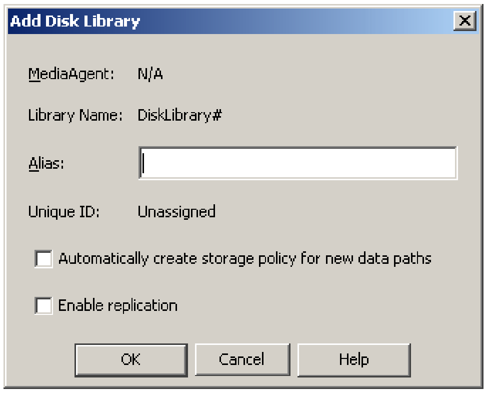
Enable Replication: For Disk Library Replication solution, select this option to use ContinuousDataReplicator to replicate data between the source (shared folder added in Step 4) and the destination (shared folder added in Step 6) mount paths. Leave this option unselected if you are using a third party application to replicate data between shared folders.

Selecting this option will automatically create a new replication set and a replication pair under ContinuousDataReplicator, when a mount path is added to this library. These replication sets and replication pairs can be monitored from the CommCell Console. It is highly recommended not to change the default settings of the replication sets, or delete the replication sets when the replication is in progress.

NOTES:

- If this option is selected, make sure to install the ContinuousDataReplicator package on the source and the destination computers before adding mount path to this library.

Click **OK**.


Add Disk Library

MediaAgent: N/A

Library Name: DiskLibrary#

Alias:

Unique ID: Unassigned

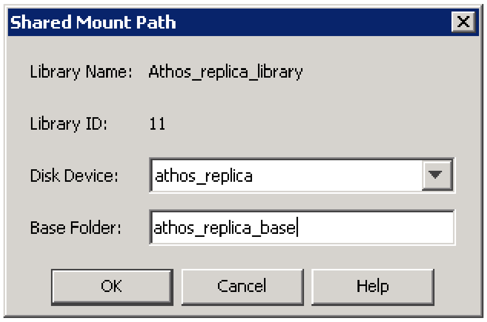
☐ Automatically create storage policy for new data paths

☐ Enable replication

12. In the **Shared Mount Path** dialog box, select the disk device that you wish to associate as the mount path from the **Disk Device** list.

In the **Base Folder** box, type the name of the base folder under which the mount path can store data. Do not include the drive letter while adding the name of the base folder.

Click **OK**.


Shared Mount Path

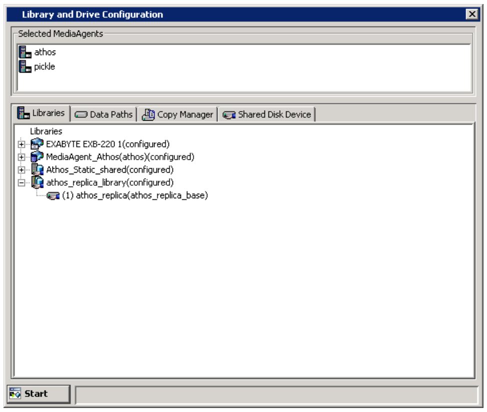
Library Name: Athos_replica_library

Library ID: 11

Disk Device: athos_replica

Base Folder: athos_replica_base

The disk library is configured.


Library and Drive Configuration
Selected MediaAgents
athos
pickle
Libraries
Data Paths
Copy Manager
Shared Disk Device
Libraries
EXABYTE EXB-220 1(configured)
MediaAgent_Athos(athos)(configured)
Athos_Static_shared(configured)
athos_replica_library(configured)
(1) athos_replica(athos_replica_base)
Start

Disk Libraries - How To

Topics | Configure | How To | Troubleshoot | Related Topics

Shared Disk Libraries

View or Modify the Device Properties for Disk Libraries with Static Mount Paths

View or Modify the Properties of Disk Devices in a Shared Mount Path

Modify the Access Information for a Shared Disk

Deconfigure a Shared Disk Device

Configure Multiple MediaAgents for a Static Shared Disk Device

Deconfigure Multiple MediaAgents for a Shared Disk Device

Disk Libraries on Replicated Disks

View the Device Paths associated with the Mount Path - See View or Modify the Properties of Disk Devices in a Shared Mount Path

Change the Access Type (Read / Write) for a Mount Path - See View or Modify the Properties of Disk Devices in a Shared Mount Path

Common - Administering Disk Libraries

Establish the Low Watermark for a Disk Library

Configuring a Low Disk Space Alert

Configure the Size of Disk Volumes

Modify the Mount and Unmount Timeouts for Disk Libraries

Create Read-Only Archive Files on filers

Enable Single Instancing of Data on a Disk Library

Enable or Disable the Disk Library

View the Disk Library Offline Reason

Establish the Mount Path Allocation Policy for a Disk Library

Establish the Mount Path Usage for a Disk Library

Enable Managed Disk Space for Disk Data

View a List of Storage Policies Accessing the Disk Library

Migrate a Disk Library

Deconfigure a Disk Library

Common - Administering Mount Paths

Add or Modify a Mount Path

Add Automated Mount Path Detection

Enable Unbuffered I/O on a Mount Path

Enable or Disable a Mount Path

View the Mount Path Offline Reason

Establish Maximum Space Allocation on a Mount Path

Reduce Data Fragmentation on a Mount Path

Perform Fragmentation Analysis

View the Contents of a Mount Path

Delete the Contents of a Mount Path

Prevent Accidentally Deleting Mount Path Contents

Move a Mount Path

Retire a Mount Path

Delete a Mount Path

View or Modify the Device Properties for Disk Libraries with Static Mount Paths

To modify the device properties for disk libraries with static mount paths:

1. From the CommCell Browser, right-click a mount path for which you wish to view the modify the properties, and then click **Properties**.
2. If necessary you can:
   - Change the **Device Alias Name**
   - Enable or disable the device by selecting or clearing the **Device Enabled** option.
3. Click **OK** to save the changes.

View or Modify the Device Properties for Disk Libraries with Static Mount Paths

To modify the device properties for disk libraries with static mount paths:

1. From the CommCell Browser, right-click a mount path for which you wish to view the modify the properties, and then click **Properties**.
2. If necessary you can:
   - Change the **Device Alias Name**
   - Enable or disable the device by selecting or clearing the **Device Enabled** option.
3. Click **OK** to save the changes.

View or Modify the Properties of Disk Devices in a Shared Mount Path

To view or modify the properties of Disk Devices in a shared mount path:

1. From the CommCell Browser, right-click a mount path for which you wish to view the MediaAgents, and then click **Properties**.
2. Click the Device Paths tab of the **Mount Path Properties** dialog box.

   You can change the Maximum number of writers by clicking the **Edit** button.

   You can enable or disable the MediaAgent's access to the device by selecting or clearing the enabled button.

   On mount paths associated with replicated disks, you can modify the read-write access to the mount path. This should not be done for Disk Libraries on Replicated Disks used for the Disk Library Replication solution.

Modify the Access Information for a Shared Disk

MODIFY THE ACCESS PATH FOR ALL MEDIAAGENTS SHARING THE DEVICE (SUPPORTED FOR WINDOWS MEDIAAGENTS)

1. Display the Library and Drive Configuration window.
2. Click the **Shared Disk Device** tab.
3. Right-click the Device that you want to modify and then click **Set Network Access Info for all Windows MediaAgents**.
4. Make the necessary changes in the Sharing Folder Properties dialog box and click **OK** to save the changes.

MODIFY THE ACCESS PATH FOR THE INDIVIDUAL MEDIAAGENTS

1. Display the Library and Drive Configuration window.
2. Click the **Shared Disk Device** tab.
3. Locate the device and then navigate to the individual folder.
4. Right-click the Folder and then click **Properties**.
5. Make the necessary changes in the Sharing Folder Properties dialog box and click **OK** to save the changes.
6. Repeat steps 4 and 5 for all the folders (MediaAgents) sharing the device.

MODIFY THE ACCESS TYPE FOR SHARED DISK DEVICE

On mount paths associated with replicated disks, you can modify the read-write access to the mount path. This should not be done for Disk Libraries on

Replicated Disks used for the Disk Library Replication solution.

Use the following steps to modify the access type for a Shared Disk Device:

1. From the CommCell Console, click the **Tools** menu and then click **Control Panel**.
2. From the **Control Panel**, double-click the **Library & Drive Configuration**.
3. From the **Select MediaAgents** dialog box, perform the following:
   - From the **Available MediaAgents** list, select the **MediaAgents** of same operating system type.
   - Click **Add >>** to move the MediaAgents to the **Selected MediaAgents** list box.
   - Click **OK**.
4. Click **OK**.
5. From the **Library and Drive Configuration** window, click the **Shared Disk Device** tab.
6. Locate the **Device** and then navigate to the individual folder.
7. Right-click the ***<Mount Path>*** and then click **Properties**.
   - If access type is selected as Read, then that mount path will be used only for read operations.
   - If access type is selected as Read/Write, then that mount path is used for both read and write operations.
8. Click **OK** to save the changes.

DECONFIGURE A SHARED DISK DEVICE

Before you Begin

- Be certain that the mount paths using the device are deconfigured. See Deleting a Mount Path for more information.

To deconfigure a shared disk device::

1. Display the Library and Drive Configuration window.
2. Click the **Shared Disk Device** tab.
3. Right-click the disk device that you wish to deconfigure, and then click **Deconfigure**.
4. Click **Yes** in the **Confirm Deconfigure** prompt.

The device is deconfigured.

NOTES

- After rebooting all the MediaAgents which shares this disk, the disk will be available for other applications.

CONFIGURE MULTIPLE MEDIAAGENTS FOR A STATIC SHARED DISK DEVICE

Use the following steps to configure multiple MediaAgents for a Shared Disk Device:

1. From the CommCell Console, click the **Tools** menu and then click **Control Panel**.
2. From the **Control Panel**, double-click the **Library & Drive Configuration**.
3. From the **Select MediaAgents** dialog box, perform the following:
   - From the **Available MediaAgents** list, select the **MediaAgents** of same operating system type.
   - Click **Add >>** to move the MediaAgents to the **Selected MediaAgents** list box.
   - Click **OK**.
4. Click **OK**.
5. From the **Library and Drive Configuration** window, click the **Shared Disk Device** tab.
6. Expand the **Device** to which you want to configure multiple MediaAgents.
7. Right-click the ***<Mount Path>*** and then click **Configure for All Selected MediaAgents**.
   - For Windows, configure all MediaAgents when the mount path is configured as UNC path and all selected MediaAgents have access to this UNC path.
   - For Unix, ensure that the directory path to be mounted in the unconfigured MediaAgents has the same directory path as that of the configured MediaAgent.
8. Click **Yes**.

The device is configured with the list of selected MediaAgents.

DECONFIGURE MULTIPLE MEDIAAGENTS FOR A SHARED DISK DEVICE

Use the following steps to deconfigure multiple MediaAgents for a Shared Disk Device:

1. From the CommCell Console, click the **Tools** menu and then click **Control Panel**.
2. From the **Control Panel**, double-click the **Library & Drive Configuration**.
3. From the **Select MediaAgents** dialog box, perform the following:
   - From the **Available MediaAgents** list, select the **MediaAgents** of same operating system type.
   - Click **Add >>** to move the MediaAgent(s) to the **Selected MediaAgents** list box.
   - Click **OK**.
4. Click **OK**.
5. From the **Library and Drive Configuration** window, click the **Shared Disk Device** tab.
6. Right-click the **Device** and then click **Deconfigure for All Selected MediaAgents**.
7. Click **Yes**.

The device is deconfigured with the list of selected **MediaAgents**.

ESTABLISH THE LOW WATERMARK FOR A DISK LIBRARY

Related Topic

Modify the low watermark

Required Capability: Capabilities and Permitted Actions

To establish the low watermark for a disk library:

1. From the CommCell Browser, right-click the disk library for which you wish to establish the low watermark, and then click **Properties**.
2. In the **Low Watermark** box, type or select the minimum percentage of free space at which the low watermark warning should be generated.

   If the amount of free space, for all the combined mount paths, reaches or falls below the low watermark, the MediaAgent displays a message in the Event Viewer and sends an Alert, if configured.

CONFIGURING A LOW DISK SPACE ALERT

Related Topics

Configure a Low Disk Space Alert

Alerts and Monitoring - How To

Required Capability: Capabilities and Permitted Actions

To configure a Low Disk Space Alert:

1. From the **Tools** menu in the CommCell Console, click **Control Panel**.
2. Double-click **Media Management**.

   The Media Management Configuration dialog box appears.
3. On the **Service Configuration** tab, set the **Number of days in advance to trigger alert for low disk space for disk library** option to a value greater than 0.

   This value is the number of days that you want to be notified before the library runs out of disk space. For example, if you want to be notified five days before the library runs out of disk space, set the value to 5.

   If the value is set to 0, then the alert is generated when the low watermark is reached.
4. Click **OK**.
5. In the Control Panel, double-click **Alerts**.

The Alerts dialog box appears.

6. Click **Add**.

   The Add Alerts Wizard appears.

7. Configure the alert according to your needs. As you configure the alert, make sure that the following options are set:
   - On the **General Information** page, set **Category** = **Media Management** and **Type** = **Library Management**.
   - On the **Threshold and Notification Criteria Selection** page, select the **Insufficient Storage** check box.
8. Once you configure the alert completely, click **Finish**.
9. Click **OK**.

CONFIGURE THE SIZE OF DISK VOLUMES

Required Capability: Capabilities and Permitted Actions

To configure the size of disk volumes:

1. From the **Tools** menu in the CommCell Console, click **Control Panel**.
2. Double-click **Media Management Configuration**.
3. Select Service Configuration tab.
4. Modify the **Disk volume physical size high watermark in GB** parameter as required.
5. Click **OK** to save the changes.

MODIFY THE MOUNT AND UNMOUNT TIMEOUTS FOR DISK LIBRARIES

Related Topic

- Configure Timeouts

Required Capability: See Capabilities and Permitted Actions

To modify the mount and unmount timeouts for disk libraries:

1. From the CommCell Browser, right-click the disk library for which you wish to change mount and unmount timeout periods, and then click **Properties**.
2. In the **Mount** and **Unmount** box, type or select the timeout periods.
3. Click **OK** to save the changes.

CREATE READ-ONLY ARCHIVE FILES ON FILERS

Related Topic

- Configure Archive Files as read only

Required Capability: Capabilities and Permitted Actions

To create read-only archive files in a disk library on filers:

1. From the CommCell Browser, right-click the disk library for which you wish to create read-only archive files, and then click **Properties**.
2. From the General tab of Library Properties, click the **Mark Archive Files as Read-Only** option.
3. Click **OK** to save the changes.

NOTES

- This option will only affect files that are subsequently created by data protection and auxiliary copy operations to this library. Permission to files that are already available in this library will not be affected.

ENABLE SINGLE INSTANCING OF DATA ON A DISK LIBRARY

Related Topic

- Enable Support for Single Instancing of Data (Content Address Storage)

Required Capability: Capabilities and Permitted Actions

To enable single instancing of data on a disk library:

1. From the CommCell Browser, right-click the disk library for which you wish to establish the single instancing of data, and then click **Properties**.
2. Click the Mount Paths tab. Note that mount paths enabled with hardware single instancing must be less than 100 characters long. Otherwise hardware single instancing might not be employed successfully.
3. Click the **Disks within this library support hardware single instancing** option.
4. Click **OK** to save the information.

ENABLE OR DISABLE THE DISK LIBRARY

Required Capability: Capabilities and Permitted Actions

To enable or disable a disk library:

1. From the CommCell Browser, right-click the disk library that you wish to enable or disable, and then click **Properties**.
2. From the General tab of Library Properties, click the **Enable Library** option.
3. Click **OK** to save the changes.

VIEW THE DISK LIBRARY OFFLINE REASON

To view the offline reason for a disk library:

1. From the CommCell Browser, right-click the disk library for which you wish to view the offline reason, and then click **Properties**.

   Information on the disk library offline reason is displayed in the **Offline Reason** box.

ESTABLISH THE MOUNT PATH ALLOCATION POLICY FOR A DISK LIBRARY

Related Topic

- Establish the Mount Path Allocation Policy for the Library

Required Capability: Capabilities and Permitted Actions

To establish the Mount Path Allocation Policy for a disk library:

1. From the CommCell Browser, right-click the disk library for which you wish to establish the mount path allocation policy, and then click **Properties**.
2. Click the Mount Paths tab.
3. Click either the **Maximum Allowed Writers** option or the **Allocate No. of Writers** option and then select the maximum number of writers.
4. Click **OK** to save the information.
5. From the CommCell Browser, right-click the mount path within the disk library and then click **Properties**.
6. Click the Allocation Policy tab.
7. Click either the **Maximum Allowed Writers** option or the **Allocate No. of Writers** option and then select the maximum number of writers.
8. Click **OK** to save the changes
9. Repeat steps 5, 6, 7 and 8 in all the mount paths associated with the disk library. Keep in mind that the sum of the writers allocated in the mount paths should be equal to the total mount paths allocated in the disk library.

ESTABLISH THE MOUNT PATH USAGE FOR A DISK LIBRARY

Related Topic

- Establish the Parameters for Mount Path Usage

Required Capability: Capabilities and Permitted Actions

To establish the Mount Path Usage for a disk library:

1. From the CommCell Browser, right-click the disk library for which you wish to establish the mount path allocation policy, and then click **Properties**.

2. Click the Mount Paths tab.
3. Click either the **Fill and spill mount paths** or the **Spill and fill mount paths** options.
4. Click **OK** to save the information.

ENABLE MANAGED DISK SPACE FOR DISK DATA

Related Topics

- Thresholds for Managed Disk Space

Required Capability: See Capabilities and Permitted Actions

To enable managed disk space for disk data:

1. Right-click the storage policy copy for which you wish to enable or disable Data Aging, and then click **Properties**.
2. From the Retention tab of the **Copy Properties** dialog box, select the **Enable Managed Disk Space for disk data** option and click **OK**.
3. From the Mount Paths tab of the **Library Properties** dialog box, set the start and stop data aging disk capacity thresholds in the **Start aging when data occupied on disk is n %** and the **Stop aging when data occupied on disk is n %** boxes, and click **OK** to save changes.

VIEW A LIST OF STORAGE POLICIES ACCESSING THE DISK LIBRARY

To view the list of Storage Policy accessing the disk library:

1. From the CommCell Browser, right-click the disk library for which you wish to view the storage policies, and then click **Properties**.
2. Click the Associations tab.

   All the Storage Policies and the Storage Policy Copies accessing the disk library are displayed.

MIGRATE A DISK LIBRARY

Required Capability: See Capabilities and Permitted Actions

Before you Begin:

Make sure that your disk library meets the appropriate criteria. For more information, see Migrate Magnetic Libraries.

To perform a disk library migration from one MediaAgent to another MediaAgent:

1. Right-click the disk library that you want to migrate to another MediaAgent and click **Migrate Disk Library**.
2. A message is displayed indicating that this operation migrates the disk library to another MediaAgent. Click **OK**.
3. The Select MediaAgent dialog box is displayed. This dialog box displays the current MediaAgent that the disk library is associated with and allows you to select a MediaAgent to migrate to. From the drop-down list, select the MediaAgent you want to migrate to and click **OK**.
4. The disk library will now be associated with the selected MediaAgent. To view the disk library properties to verify successful migration, right click on the disk library where you want to view the properties, and click **Properties**.

   The MediaAgent is displayed on the **General** tab.
5. Make sure that the mount path associated with the disk library, points to valid path. (See Add or Modify Mount Paths for step-by-step instructions.)

DECONFIGURE A DISK LIBRARY

Data associated with a library will be lost, when it is deconfigured.

Before you Begin

- Be certain that the library that you want to remove is not in use. Use the Job Controller to find and kill any jobs that use the library.
- Make sure that every storage policy copy associated with the library has been deleted. Determine the storage policies accessing the library as described in View the Storage Policies Accessing a Library.

To deconfigure a disk library:

1. Display the Library and Drive Configuration window.

2. Right-click the library that you want to deconfigure, and then click **Deconfigure**.
3. A prompt appears, reminding you that the library's storage policy copies must be deleted in order for the library to be deconfigured. If no storage policy copies are associated with the library and you want to deconfigure, click **Yes**.

   The disk library is removed from the `Library and Drive Configuration` window.

ADD OR MODIFY A MOUNT PATH

Required Capability: Capabilities and Permitted Actions

To add or modify a mount path to an existing disk library:

1. Display the Library and Drive Configuration window.
2. Select the library to which you want to add a mount path, right-click, and then select **Add Mount Path**.
3. In the Add Mount Path dialog box, select either **Local Path** or **Network Path**.
4. If you select **Local Path**, click **Browse** to select a mount path, or enter a mount path.
5. If you select **Network Path**, type the user name and password to access the network share. Click **Browse** to select a mount path, or enter a mount path.
6. Click **OK**. The mount path is added to the specified location.

ADD AUTOMATED MOUNT PATH DETECTION

To add automated mount path detection to an existing disk library:

1. Display the Library and Drive Configuration window.
2. Select and right-click the library, and then select **Add Automated Mount Path Detection**.
3. From the **MediaAgent** list, select the MediaAgent.
4. In the **Folder** box, type the mount path or click **Browse [...]** to select a mount path.

   > If you need to share the volumes across MediaAgents, share the mount folder. This will automatically share the newly added volumes.

5. If you wish to configure mount path for all selected MediaAgent(s), perform the following:
   - Select **Configure for all other selected Windows MediaAgents** check box.
   - In the **Connect As** box, specify the user account information.
   - In the **Password** box, specify the password to access the mount path.
   - In the **Verify** Password, re-type the password.
   - In the **Folder** box, type the mount path or click **Browse [...]** button to select a mount path.
   - Select **Read Only** check box, to give read only permission to the mount path.

   The libraries will be shared between all MediaAgents as per the mount folder specified at the time of configuration.
6. Click **OK**.

ENABLE UNBUFFERED I/O ON A MOUNT PATH

Related Topic

- Use Unbuffered I/O

Required Capability: Capabilities and Permitted Actions

To enable unbuffered I/O on a mount path:

1. From the CommCell Browser, right-click the mount path that you wish to enable unbuffered I/O, and then click **Properties**.
2. From the General tab of Library Properties, click the **Use unbuffered I/O** option.
3. Click **OK** to save the changes.

Enable or Disable a Mount Path

Required Capability: Capabilities and Permitted Actions

To enable or disable a mount path:

1. From the CommCell Browser, right-click the mount path that you wish to enable or disable, and then click **Properties**.
2. From the General tab of Library Properties, click the **Enable MountPath** option.
3. Click **OK** to save the changes.

View the Mount Path Offline Reason

To view the offline reason for a mount path:

1. From the CommCell Browser, right-click the mount path for which you wish to view the offline reason, and then click **Properties**.

   Information on the mount path offline reason is displayed in the **Offline Reason** box.

Establish Maximum Space Allocation on a Mount Path

Related Topic

- Establish Space Allocation on the Mount Path

Required Capability: Capabilities and Permitted Actions

To establish maximum space allocation on a mount path:

1. From the CommCell Browser, right-click the mount path that you wish to establish the space allocation, and then click **Properties**.
2. Click the Allocation Policy tab.
3. In the **Space Allocation** section, establish one or more of the following options:
   - Specify the minimum reserve space in the **Reserve Space** box.
   - Specify the maximum space that can be used by the mount path by choosing either the **Use until free space on mount path reaches Reserved Space** or **Do not consume more than *n* GB** options.
4. Click **OK** to save the changes.

NOTES

- In some situations the mount path may consume more space and exceed the specified minimum reserve space. Consider the following example:

  If you have established the minimum reserve space as 2 GB, and run a 2 streamed data protection operation when the disk space is 2.01 GB, both the streams will use a minimum of 25 MB before spanning to an alternate mount path. In such a situation the free space will fall below the specified 2 GB.

  This could also happen if 2 concurrent single-streamed data protection operation is initiated to the same mount path, using 2 different storage policies.

- Similarly, the system may consume more than the specified maximum space. Consider the following example:

  When a data protection job is initiated, the system checks for the available disk space and verifies whether it is less than the specified maximum space. For example if you have specified 5 GB as the maximum space and if you have used 4.75 GB, the data protection job will be initiated using the mount path. However, if the size of the data is .5 GB, the system will write the entire data. In such a situation the space consumed will be more than the specified maximum space.

  Note that a data protection operation will generally write to the mount path until the minimum reserve space is reached, before spanning to an alternate path.

Reduce Data Fragmentation on a Mount Path

Related Topic

- Reduce Fragmentation of Data on a Mount Path

Required Capability: Capabilities and Permitted Actions

To reduce data fragmentation a mount path:

1. From the CommCell Browser, right-click the mount path that you wish to establish the space allocation, and then click **Properties**.
2. Click the Allocation Policy tab.

3. In the **Fragmentation** section, click and select the **Minimize fragmentation by allocating write blocks of *n* MB** option and specify the size that must be pre-allocated for each write operation in the box.
4. Click **OK** to save the changes.

PERFORM FRAGMENTATION ANALYSIS

Related Topic

- Fragmentation Analysis

Required Capability: Capabilities and Permitted Actions

➤ To execute disk library maintenance on selected mount paths:

1. Right-click the disk library containing the mount paths you wish to execute disk library maintenance and click **Fragmentation Analysis**.
2. From the Disk Library Maintenance window, select the desired mount paths in the **Analysis** check box.
   - Click **OK** to execute the maintenance job immediately.
   - Click **Schedule** to schedule the job. From the Schedule Details tab, select the necessary scheduling option. Click **OK** to save the schedule.

VIEW THE CONTENTS OF A MOUNT PATH

Required Capability: Capabilities and Permitted Actions

➤ To view the contents of a mount path

1. From the CommCell Browser, right-click the mount path for which you wish to view the content, and then click **View Contents**.

   or

   From the Media Used By Job ID dialog box right-click the media for which you wish to view the content, and then click **View Contents**.
2. The Contents of Media dialog box displays the details of jobs available in the media.

DELETE THE CONTENTS OF A MOUNT PATH

Required Capability: Capabilities and Permitted Actions

➤ To delete the contents of a mount path:

1. From the CommCell Browser, right-click the mount path for which you wish to delete the contents, and then click **Delete Contents**.
2. Click **Yes** in the Warning prompt to continue.

   Click **No** to abort the operation.
3. In the **Enter Confirmation text** dialog box, type `erase and reuse media` and then click **OK**.

   Click **Cancel** to abort the operation.

NOTES

This operation deletes the data from the CommServe database. Note that this operation does not free-up the disk space in the mount path. A Data Aging operation must be run subsequently to free-up the disk space.

PREVENT ACCIDENTALLY DELETING MOUNT PATH CONTENTS

This feature is not supported on some libraries and may need to be turned off.

Required Capability: Capabilities and Permitted Actions

➤ To prevent accidentally deleting the contents of mount paths:

1. From the CommCell Browser, right-click the library you wish to protect and then click **Properties**.
2. In the Mount Path tab, select **Prevent accidental deletion of data from mountpaths** to enable the feature. Clear this option to disable the feature.
3. Click **OK**. Contents of mount paths created when this option is enabled are protected from accidental deletion.

MOVE A MOUNT PATH

The following procedure describes the step involved in moving a mount path currently associated with a disk library.

To move a mount path:

1. Copy the `CV_MAGNETIC` folder (including its contents) from the current mount path location, to the new mount path location.
2. From the CommCell Console: Display the Library and Drive Configuration window.
3. Locate the disk library for which you wish to move the mount path.
4. Right-click the mount path that you wish to move and then select **Properties**.
5. From the Mount Path Properties dialog box, enter the new path.
   - If you select **Local Path**, click **Browse** to select a mount path, or enter a mount path.
   - If you select **Network Path**, type the user name and password to access the network share. Click **Browse** to select a mount path, or enter a mount path.
6. Click **OK** to save the information.

   The mount path is moved to the specified location. Verify that the mount path is online and accessible after the move.

RETIRE A MOUNT PATH

The following procedure describes the step involved in retiring or phasing out a mount path from a disk library.

To retire a mount path:

1. From the CommCell Browser, right-click the mount path that you no longer want to use, and then click **Properties**.
2. Click the Allocation Policy tab.
3. Choose the **Disable mount path for write** option.
4. Click **OK** to save the changes.
5. If necessary, create a new mount path for subsequent operations by following the procedure for Add Mount Paths.

NOTES

- When you **Disable mount path for write** operations, the mount path will not be used for subsequent write operations. You can however perform read operations on the data available in the mount path.
- Depending on the retention criteria set for the storage policy copy that was used to write the data, the data in the mount path will be pruned when data aging operation is performed.
- If you wish to delete the mount path, use **Valid Data** in the Mount Path Properties (General) tab to determine whether the mount path has valid data.

DELETE A MOUNT PATH

A mount path can only be deleted if it does not contain backup data and is not the last remaining mount path. You can remove backup data either by deleting all storage policy copies that point to the disk library, or by taking the mount path offline, allowing its data to age and then running the Data Aging operation. Before you can delete a storage policy copy, all subclients associated with the copy must either be associated with a different storage policy copy or deleted.

To delete a mount path:

1. Delete the contents of the mount path as described in Delete the Contents of a Mount Path. Note that once data is deleted on disk mount paths, it will not be restorable.
2. Display the Library and Drive Configuration window.
3. Select the mount path that you want to delete, right-click, and then select **Delete Mount Path**.
4. Click **OK** in the prompt that appears, confirming the deletion of the mount path.

   The mount path is removed from the **Library and Drive Configuration** window display.

Optical Libraries

Topics | Related Topics

OVERVIEW

You can configure optical libraries attached to a MediaAgent running on a Windows platform. Optical libraries with or without barcode readers can be configured. However, optical libraries (with or without barcode reader) can be configured only on Windows 2000, Windows 2003 servers, and Windows 2008 servers (32 bit, x64, and R2 editions).

Both the configuration and operations in an optical library are similar to that of a tape library. The following sections describe the issues that are specific to the optical libraries.

All the library, drive and media operations in an optical library are similar to that of a tape library. Refer to the following sections for more information:

- Library Operations
- Drive Operations
- Media Operations
- Hardware Maintenance

OPTICAL LIBRARY CONFIGURATION

The optical library must be attached to a MediaAgent running on a Windows server computer. The library and/or drives can be connected through SCSI adaptors. We recommend to connect no more than four drives per SCSI card.

Observe the following guidelines while configuring optical libraries

- The latest firmware version should be loaded to the library.
- Use all optical drives with the same speed and optical cartridges of same capacity.
- Do not set the data-protect tab on any cartridge. Setting the data-protect tab will fail all operations on the cartridge.
- Disable the library's media changer in the Windows Device Manager as described in the Driver Configurations.
- Also make sure that the `Removable Storage service` is disabled.
- Libraries containing UDO and DVD media will be configured as blind libraries.

The optical library can be configured using one of the following configurations:

- Direct-attached library (See Direct-Attached Libraries for more information.)
- Direct-attached shared library (See Direct Attached Shared Libraries for more information.)

If the optical library does not have a barcode reader, you can configure the library as a blind library. (See Blind Libraries for more information.)

BEST PRACTICES FOR OPTICAL LIBRARIES

Observe the following guidelines while using the optical libraries:

- Do not explore or browse any Removable Disk (X:) which corresponds to an optical drive in the optical library. Doing so may lock the drive for data access and may result in data corruption.
- Do not have volume management services from other software vendors running. This would interfere with the MediaAgent software in terms of managing the optical platters.

PnP (Plug and Play) Disk Libraries

Topics | Configure | How To | Troubleshoot | Related Topics

OVERVIEW

In locations where it is hard to configure and manage tapes due to operational issues Plug and Play (PnP) storage devices (e.g., FireWire, USB, SATA storage devices, etc.) can be used for storage instead of tapes. Once configured, PnP disks are treated like tapes in a Stand-Alone drive.

Disk devices that do not retain the Operating System drive letter when disconnected/unloaded can be configured as PnP disk libraries (for example, thumb drives, etc.).

> Support for devices like USB, FireWire, SATA storage devices is not dependant on any specific vendor make or model. These devices are considered supported as long as the host operating system appropriately detects the devices as disk targets. Therefore, these device types are not listed within the Hardware Compatibility Matrix.

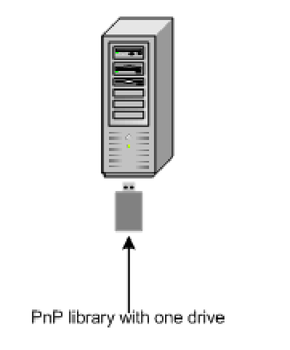
The following sections provide a detailed discussion on the features associated with PnP Disks.

CONFIGURING PNP DISK LIBRARIES

To use a PnP disk, you must first configure a library in the MediaAgent in which you plan to use the device. Note that only one PnP library can be configured per MediaAgent. Although multiple drives can be configured, only single-streamed jobs are supported. (Multiple drives provide the ability to span across multiple media for a single-streamed job.)

See Configure a PnP Disk Library for step-by-step instructions on configuring a PnP library.

Single PnP Disk Configuration



SUPPORTED FEATURES

Once configured, PnP Disk Libraries are similar to a stand-alone drive and all the features, including the following are supported by these libraries:

- Automatic Labeling Schemes
- Manual Stamping of Media

> For PnP libraries, Manual Stamping of Media is supported for libraries that have only one USB drive. It is not supported for PnP libraries that have multiple USB drives.

In addition, the following options specific to PnP Disk Libraries are also available available in the **Library Properties - Media Usage** tab:

- **Only use PnP disk when it is blank**

  Enabling this option ensures that blank disks with no other data is used for data protection operations and allows you to use disks exclusively for data protection purposes. (See Enable (or Disable) Option to Only Use Blank PnP Disks for step-by-step instructions.)

- **Use disk only when the size is greater than (n) MB**

  Enabling this option and specifying the minimum disk size ensures that data protection operations use disks with a specific size. Depending on the size of your data protection operations, you can avoid using smaller disks which may result in a job spanning multiple disks.

Data aging and media recycling are supported. In addition the following operations which are similar to the stand-alone drives are also supported:

- Media Operations in Stand-Alone Drives
- Pop-up Messages in Stand-Alone Drives
- Detecting Media Changes in Stand-Alone Drives

As most of the operations supported by tape/optical libraries are also supported, refer to the following topics for specific information on the operation:

- Library Operations
- Drive Operations
- Media Operations

See also:

- MediaAgents - Supported Features, Agents and Devices for MediaAgent support of PnP Disk Libraries.

LICENSE REQUIREMENT

This feature requires a Feature License to be available in the CommServe® Server.

Review general license requirements included in License Administration. Also, View All Licenses provides step-by-step instructions on how to view the license information.

PnP (Plug and Play) Disk Libraries - Configure

Topics | Configure | How To | Troubleshoot | Related Topics

CONFIGURE A PNP DISK LIBRARY

The following procedure describes the steps involved in configuring a PnP Disk Library which will use one PnP Disk at any given time.

Required Capability: See Capabilities and Permitted Actions

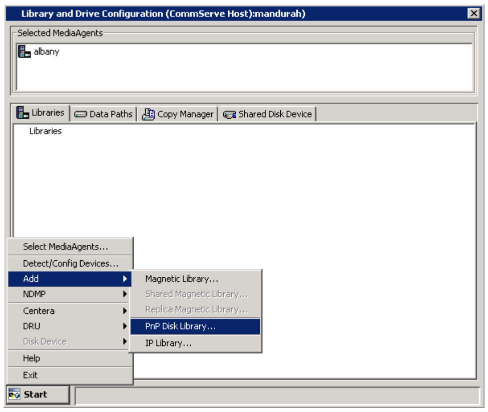
BEFORE YOU BEGIN

- Verify that the disk is visible to the Operating System
- This feature requires a Feature License to be available in the CommServe® Server.

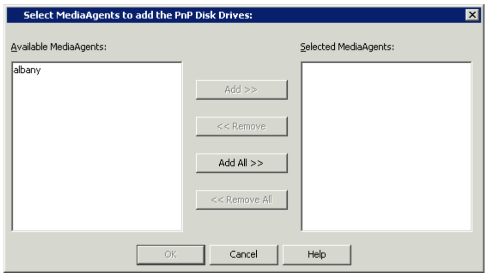
  Review general license requirements included in License Administration. Also, View All Licenses provides step-by-step instructions on how to view the license information.
- If you are using a PnP Disk Library with removable SATA drives, then you must create the required registry key bSupportPnPSATADrives and set the value to 1.

TO CONFIGURE A PNP DISK LIBRARY

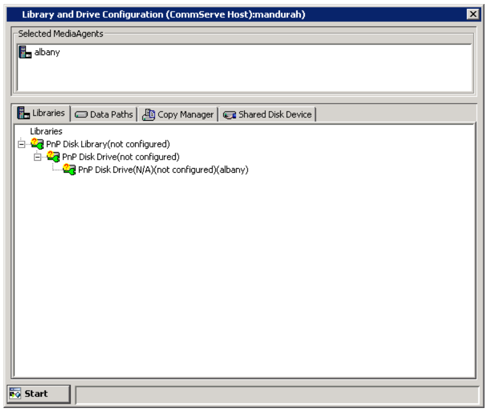
1. Display the Library and Drive Configuration window.
2. Click the **Start** menu, select **Add** and then click **Add PnP Library**.



3. Select the name of the MediaAgent in which you wish to configure the library.



The library is added and displayed in the **Library and Drive Configuration** window.


Library and Drive Configuration (CommServe Host):mandurah)
Selected MediaAgents
albany
Libraries
Data Paths
Copy Manager
Shared Disk Device
Libraries
PnP Disk Library(not configured)
PnP Disk Drive(not configured)
PnP Disk Drive(N/A)(not configured)(albany)
Start

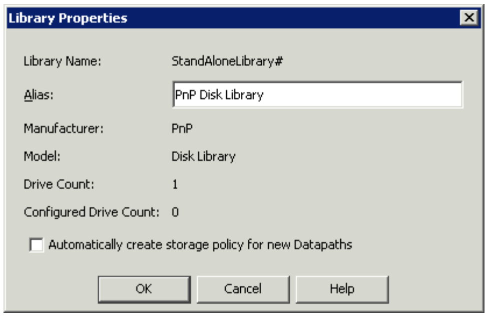
4. If necessary, right-click the library and then click **Properties**.

From the **Library Properties** dialog box, you can modify the following options:

- **Alias**: The name of the library. This name is displayed in the CommCell Browser for the library.

  We strongly recommend that you provide appropriate labels or aliases for each PnP Library. This will help you identify the proper library when you are prompted to insert media into a drive.

When you are satisfied with your changes, click **OK**.


Library Properties

Library Name: StandAloneLibrary#

Alias: PnP Disk Library

Manufacturer: PnP

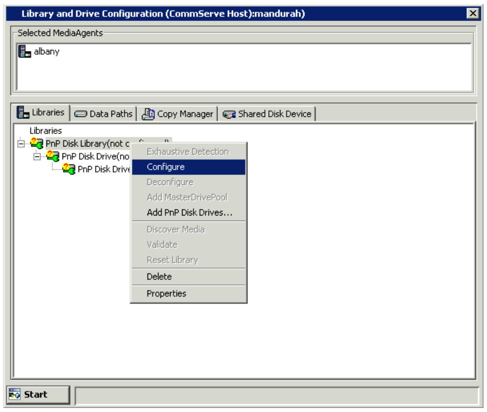
Model: Disk Library

Drive Count: 1

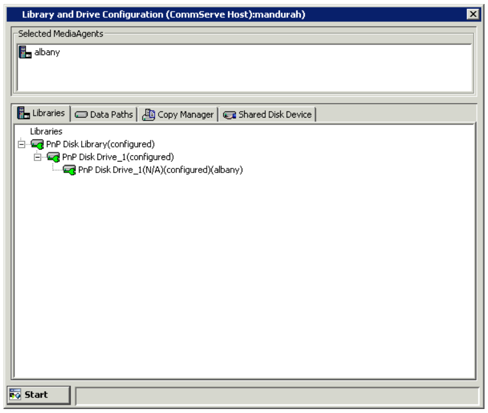
Configured Drive Count: 0

☐ Automatically create storage policy for new Datapaths

5. Right-click the library and then click **Configure**.



The status of the library changes to `configured`.


Library and Drive Configuration (CommServe Host):mandurah)
Selected MediaAgents
albany
Libraries
Data Paths
Copy Manager
Shared Disk Device
Libraries
PnP Disk Library(configured)
PnP Disk Drive_1(configured)
PnP Disk Drive_1(N/A)(configured)(albany)
Start

PnP (Plug and Play) Disk Libraries - How To

Topics | Configure | How To | Troubleshoot | Related Topics

PnP Disk Specific Options

- Enable (or Disable) Option to Only Use Blank PnP Disks
- Enable (or Disable) the Option to Use PnP Disks with a Specific Size

Media Labeling

- Create Automatic Labeling Schemes
- Add Media Identifiers (Stamp Media)

Detecting Media Changes

- Setup Automatic Checking of Media
- Verify Media
- Enable (or Disable) Automatic Use of Spare Media from Different Scratch Pools

Other Options

- Enable (or Disable) Media Related Pop-Ups in the CommCell Console

Enable (or Disable) Option to Only Use Blank PnP Disks

Required Capability: See Capabilities and Permitted Actions

To enable (or disable) option to only use blank PnP Disks :

1. From the CommCell Browser, right-click the library for which you wish to modify this parameter and then click **Properties**.
2. Click the Media Usage tab.
3. Click **Only use PnP disk when it is blank** option.
4. Click **OK** to save the changes.

Enable (or Disable) Option to Use PnP Disks with a Specific Size

Required Capability: See Capabilities and Permitted Actions

To senable (or disable) option to use PnP disks with a specific size:

1. From the CommCell Browser, right-click the library for which you wish to modify this parameter and then click **Properties**.
2. Click the Media Usage tab.
3. Click **Use disk only when the size is greater than** option and specify the size in MB.
4. Click **OK** to save the changes.

CREATE AUTOMATIC LABELING SCHEMES

Related Topic

- Automatic Labeling Schemes

Required Capability: See Capabilities and Permitted Actions

▶ To create automatic labeling schemes for stand-alone drives:

1. From the CommCell Browser, right-click the library for which you wish to create the labeling schemes and then click **Properties**.
2. Click the Media tab.
3. From the **Barcode Labeling Scheme** region, select the label and then click **Add Token**. The selected label is displayed in the box at the bottom of the region.
4. Click **OK** to save the changes.

ADD MEDIA IDENTIFIERS (STAMP MEDIA)

Required Capability: See Capabilities and Permitted Actions

▶ To add media identifiers for media associated with stand-alone drives:

1. From the CommCell Browser, right-click the library (stand-alone drive or PnP drive) for which you wish to add the identifiers, and then click **Stamp Media**.
2. In the Stamp Media dialog box specify whether the labeling scheme should be used or enter the barcode number or a unique identifier for the media.
3. Click **OK**.

   The media is listed in the **Default Scratch** pool.

SETUP AUTOMATIC CHECKING OF MEDIA

Related Topic

- Setting-Up Automatic Labeling Schemes

Required Capability: See Capabilities and Permitted Actions

▶ To setup automatic checking of media in stand-alone drives:

1. From the CommCell Browser, right-click the library for which you wish to modify this parameter and then click **Properties**.
2. Click the Drive tab.
3. Click on **Check for media change in drive every n minute(s)** option and specify the minutes.
4. Click **OK** to save the changes.

VERIFY MEDIA

Related Topic

- Detecting Media Changes in Stand-Alone Drives

Required Capability: See Capabilities and Permitted Actions

▶ To verify media in stand-alone drives:

1. From the CommCell Browser, right-click the media in the stand-alone drive and then click **Verify Media**.
2. The system verifies the media and then displays the media information in the **Verify Media** dialog box. Click **OK** to close the dialog box.

ENABLE (OR DISABLE) AUTOMATIC USE OF SPARE MEDIA FROM DIFFERENT SCRATCH POOLS

Required Capability: See Capabilities and Permitted Actions

▶ To enable (or disable) automatic use of spare media from different scratch pools:

1. From the CommCell Browser, right-click the library for which you wish to enable or disable this option then click **Properties**.

2. Click the Media tab.
3. Select the **Automatically use spare media from different scratch pool if found in drive** to enable the option, or clear the option to disable it.
4. Click **OK** to save the changes.

Enable (or Disable) Media Related Pop-Ups in the CommCell Console

Related Topics:

- Pop-up Messages in Stand-Alone Drives

Required Capability: See Capabilities and Permitted Actions

To enable (or disable) media related pop-ups in the CommCell Console:

1. From the CommCell Browser, right-click the library for which you wish to enable or disable the pop-ups then click **Properties**.
2. Click the Media tab.
3. Click on **Show Media related pop-up messages on CommCell Console** to enable the option, or clear the option to disable it.
4. Click **OK** to save the changes.

SAN-Attached Libraries

Topics | Best Practices | Configure | How To | Troubleshoot | Related Topics

OVERVIEW

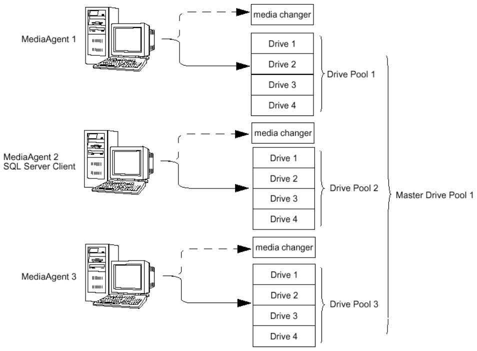
SAN environments have the following advantages:

- Reduces network traffic by directing the data over SAN, rather than the LAN.
- Enables optimal utilization of resources by enabling load-balancing between several MediaAgents and available resources.

Using Dynamic Drive Sharing (DDS), all the libraries and drives available in the SAN can be shared by the MediaAgents that have access to the SAN.

The following illustration represents a library shared via SAN with dynamic drive sharing (DDS). Three MediaAgents share a tape library with four drives.

Note that any of these MediaAgents can also be attached to additional libraries. Also the library can have additional drives which can be configured for other MediaAgents. In addition, you can also configure one or more MediaAgents as failover candidates to ensure that all the jobs using the library are performed without interruption in the event of a failure in any one MediaAgent.



In the above illustration:

- All the MediaAgents share the same four drives, using Dynamic Drive Sharing.
- Each MediaAgent has a drive pool which is grouped under one master drive pool for the library.
- The media changer can be controlled by some or all MediaAgents if they are configured as failover library controller candidates.

  Within the software, the SAN environment also provides the facility to configure multiple controllers across MediaAgents that access a library. See Library Controllers, for more information.

> **WARNING**
>
> Stop and disable Removable Storage Management (RSM) service on all Windows 2000 on a SAN, which can detect the shared tape/optical drives that are configured. These include other MediaAgents and even other machines which do not have any components installed. This is a very stringent requirement as data corruption occurs if both RSM and MediaAgent running on any machine in the SAN access the same drive at the same time.
>
> We strongly recommend that in a SAN based environment, hardware zoning of tape drives be implemented so that only the designated MediaAgents can detect and control the devices. This will minimize unnecessary monitoring and access to the devices from non-designated machines.

LIBRARY CONFIGURATION

AUTOMATIC CONFIGURATION

When multiple MediaAgents share the libraries and drives in the SAN environment, the DDS configuration process can be automated. This can done by first configuring the library in any one of the MediaAgents that share the library. Subsequently, the DDS setup is automatically established in all the other MediaAgents, without any user-interaction.

Automatically Configure Libraries Shared Across a SAN provides step-by-step instructions on how to configure multiple MediaAgents using the automatic configuration.

MANUAL CONFIGURATION

You can also manually configure the library with a DDS configuration for each of the MediaAgents sharing the library. This method of configuration, allows you to customize the configuration of library controllers on all or specific MediaAgents.

Manually Configure Libraries Shared Across a SAN provides step-by-step instructions on how to configure multiple MediaAgents using the manual configuration.

NOTES

- The option to automatically create/configure DDS DrivePools is not available for NAS-attached libraries; Dynamic Drive Sharing must be configured manually. For instructions on how to configure DDS for NAS-attached libraries, see Configure NAS-attached Libraries Shared Across a SAN .

CONFIGURING MULTIPLE HOST BUS ADAPTORS (HBA)

This feature provides the facility to configure a device with DDS using different HBAs on the same MediaAgent.

Once enabled, a MediaAgent with multiple HBA zoned to see the same drive(s) will have multiple devices (one for each HBA)appearing in the Library and Drive Configuration window. If the **Auto create DDS Drive Pool** option in **Library Properties** is enabled and if the drive(s) on any MediaAgent (local or remote) are configured, then when the MediaAgent Service are re-started, the system will automatically add one drive pool for each instance of the drive(s) as seen by the HBAs on that MediaAgent.

This feature is not supported for NAS-attached libraries.

Use the following steps to configure the device:

1. Create the DoFailoverDrivePool registry key on the CommServe.
2. Also create the DoFailoverDrivePool registry key on the MediaAgent in which you wish to configure the device.
3. If you are about to configure the library, follow the steps described in Automatically Configure Libraries Shared Across a SAN.
4. Perform the following steps if the library is already configured and you wish to create a DDS setup:
   - Display the Library and Drive Configuration window.
   - Right -click the library for which you wish to create the DDS and then click **Properties**.
   - Enable the **Auto Configure Failover Library Controllers** option.
   - Stop and restart the MediaAgent services on the MediaAgent computer.

> **WARNING**
>
> If you have more than one HBA, and you do not wish to configure the library in a DDS setup as described above, you will see more than on library when you detect the device in the **Library and Drive Configuration** window.
>
> You must configure only one of those detected libraries. Configuring all the libraries may cause undesirable results, resulting in data loss.

See Also:

- Configuring Round Robin of HBA Cards

LIBRARY CONTROLLERS

To ensure that all library related jobs are performed without interruption in the event of a failure in the MediaAgent controlling the media changer, the software provides the facility to configure the active library controller and failover library controller candidates in the MediaAgents that share a library in the SAN environment. This feature provides the following benefits:

- Automatic switching of the active library controller to the next available failover library controller candidate, in the event of a failure or non availability of the MediaAgent controlling the active library controller.
- Facility to manually switch an active library controller to the next available failover library controller candidate, if the machine hosting the active library controller has a problem or for the purpose of balancing the workload. Failover library controller setup can be configured on MediaAgents that access a library in the SAN environment.

The MediaAgent automatically switches an active library controller to the next available failover library controller candidate when the following events occur:

- The machine hosting the active library controller is powered off or not accessible due to a network failure.
- Services in the machine hosting the active library controller is not started or running.
- The MediaAgent associated with the active library controller is marked offline from the **CommCell Console**.

Back to Top

SAN-Attached Libraries - Configure

Topics | Best Practices | Configure | How To | Troubleshoot | Related Topics

AUTOMATICALLY CONFIGURE LIBRARIES SHARED ACROSS A SAN

The following procedure describes the steps involved in automatically configuring a library that is shared across a SAN with DDS, in both the clustered and non-clustered environment. This procedure does not apply to NAS-attached libraries. See Configure a Library Shared Across a SAN Environment for step-by-step instructions on configuring NAS-attached libraries.

BEFORE YOU BEGIN

Check the following before you configure the library in the SAN environment:

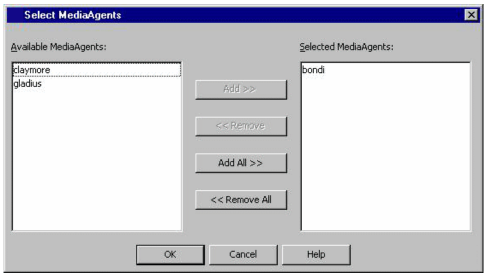
- Hardware is configured according to the conventions detailed in Hardware Configuration Guidelines - Libraries Attached to a SAN.
- MediaAgent software is installed on every computer that is connected to the SAN, and that will access the library. The MediaAgent software can be installed on the computers in any order; the installation sequence does not affect the library configuration.
- Whether the library supports the SCSI 3 drive identification information. To detect whether the library supports SCSI 3, run the **CVScsiTool.exe** available in the `<`*`Software Installation Path`*`>\Base` folder from the command prompt. If SCSI 3 is available, the **Drive Identifiers** will be displayed under **Library Information**. For detailed description of SCSI 3 drive identification, see Detection for libraries that support SCSI 3 drive identification information.
- Note the following for configuring a library attached to the MediaAgent on a cluster:
  - MediaAgent clustering can be supported only for libraries in the SAN environment.
  - Configure the MediaAgents on an active node. The active node takes care of copying the necessary configuration information to the passive nodes.
  - Ensure that both the active and passive nodes are up and running before you begin the configuration.
- This feature requires a Feature License to be available in the CommServe® Server.

  Review general license requirements included in License Administration. Also, View All Licenses provides step-by-step instructions on how to view the license information.

TO AUTOMATICALLY CONFIGURE LIBRARIES SHARED ACROSS SAN

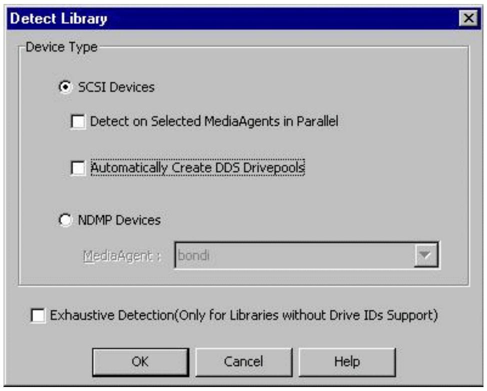
1. Display the Library and Drive Configuration window.

In the **Select MediaAgents** dialog box, select the name of *any one* MediaAgent that will share the library.

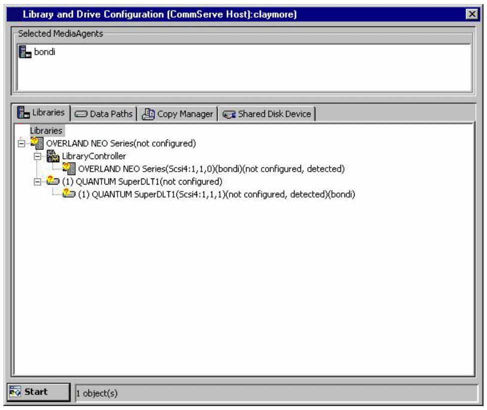


2. Detect the devices. Use Detection or Exhaustive Detection as required.

If the library supports SCSI 3 drive identification, it is not necessary to perform an exhaustive detection.


Detect Library
Device Type
● SCSI Devices
□ Detect on Selected MediaAgents in Parallel
□ Automatically Create DDS Drivepools
○ NDMP Devices
MediaAgent : bondi
□ Exhaustive Detection(Only for Libraries without Drive IDs Support)
OK
Cancel
Help

The library and all drives are displayed for the MediaAgent that is connected to the SAN in the **Library and Drive Configuration** window.



Library and Drive Configuration (CommServe Host):claymore)

Selected MediaAgents

bondi

Libraries
- OVERLAND NEO Series(not configured)
  - LibraryController
    - OVERLAND NEO Series(Scsi4:1,1,0)(bondi)(not configured, detected)
  - (1) QUANTUM SuperDLT1(not configured)
    - (1) QUANTUM SuperDLT1(Scsi4:1,1,1)(not configured, detected)(bondi)

1 object(s)

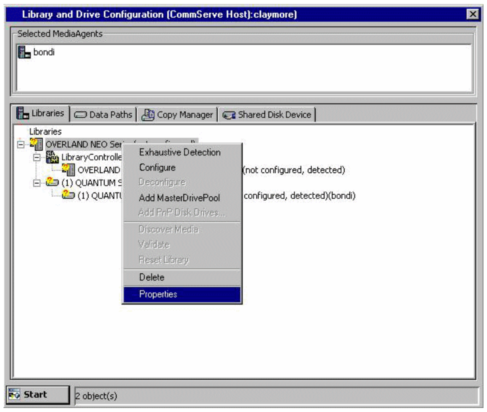
For a Solaris MediaAgent in the SAN environment, the operation will fail to detect devices with SCSI target higher than 15 and/or LUN higher than 7. In a such a situation additional entries must be added for such devices in the **wa.conf** file. For information on adding these entries see Add Additional Entries in **wa.conf** File in the Solaris MediaAgent.

For a NetWare MediaAgent, you may see a number of drives in addition to the drives that are actually present. These drives are displayed as empty slots. You can ignore these empty slots and configure the library using the drives that were detected successfully.

If any additional drives are visible on any of the MediaAgents due to incorrect zoning you must do one of the following:

- Correct the zoning and restart the configuration process.
- Delete the additional drives before performing the next step.

3. Right-click the library and then click **Properties**.



Library and Drive Configuration (CommServe Host):claymore)

Selected MediaAgents

bondi

2 object(s)

4. From the **Library Properties** dialog box, select the following option:

- **Auto Configure DDS DrivePool:** Enable this option to automatically configure the DDS drive pools for MediaAgents sharing these drives.

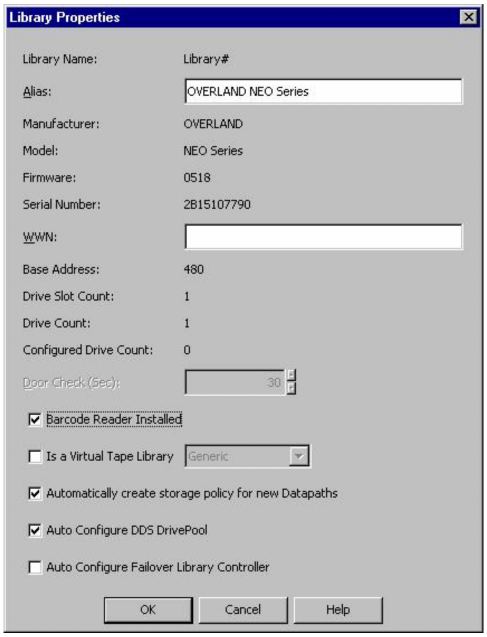
Optionally, consider the following options and enable or disable it if necessary:

- **Auto Configure Failover Library Controllers**: Enable this option to automatically configure the Failover Library Controllers in all the MediaAgents sharing this library.
- **Automatically create storage policy for new Datapaths**: Enable this option to automatically create a new Storage Policy when the library is configured.

Click **OK**.

NOTES

- The option to automatically create/configure DDS DrivePools is not available for NAS-attached libraries; Dynamic Drive Sharing must be configured manually. For instructions on how to configure DDS for NAS-attached libraries, see Configure NAS-attached Libraries Shared Across a SAN .



Library Properties

Library Name: Library#

Alias: OVERLAND NEO Series

Manufacturer: OVERLAND

Model: NEO Series

Firmware: 0518

Serial Number: 2B15107790

WWN:

Base Address: 480

Drive Slot Count: 1

Drive Count: 1

Configured Drive Count: 0

Door Check (Sec): 30

☑ Barcode Reader Installed

☐ Is a Virtual Tape Library Generic

☑ Automatically create storage policy for new Datapaths

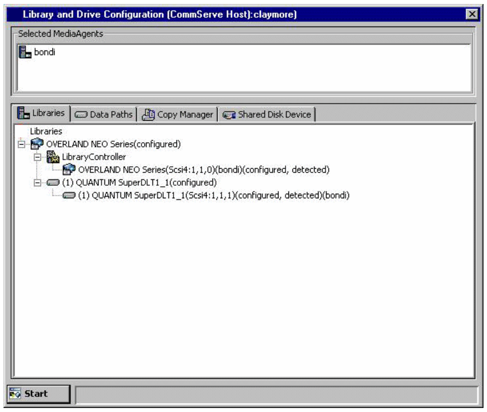
☑ Auto Configure DDS DrivePool

☐ Auto Configure Failover Library Controller

5. Configure the library as described in Configure Devices.

The library is configured and displayed with the **configured, detect success** status in the **Library and Drive Configuration** window.

The **Library** tab provides the physical view of the devices (library and drives).



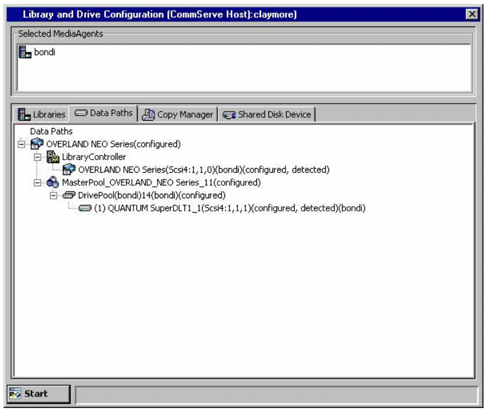
Library and Drive Configuration (CommServe Host):claymore)

Selected MediaAgents

bondi

```
Libraries
⊟ OVERLAND NEO Series(configured)
   ⊟ LibraryController
      └ OVERLAND NEO Series(Scsi4:1,1,0)(bondi)(configured, detected)
   ⊟ (1) QUANTUM SuperDLT1_1(configured)
      └ (1) QUANTUM SuperDLT1_1(Scsi4:1,1,1)(configured, detected)(bondi)
```

The **Data Paths** tab provides a logical view of the data path used to access the devices - library, master drive pool, drive pool, drive.



Library and Drive Configuration (CommServe Host):claymore)

Selected MediaAgents

bondi

```
Data Paths
⊟ OVERLAND NEO Series(configured)
   ⊟ LibraryController
      └ OVERLAND NEO Series(Scsi4:1,1,0)(bondi)(configured, detected)
   ⊟ MasterPool_OVERLAND_NEO Series_11(configured)
      ⊟ DrivePool(bondi)14(bondi)(configured)
         └ (1) QUANTUM SuperDLT1_1(Scsi4:1,1,1)(configured, detected)(bondi)
```

TO AUTOMATICALLY CONFIGURE THE DATA PATHS IN THE STORAGE POLICY COPY

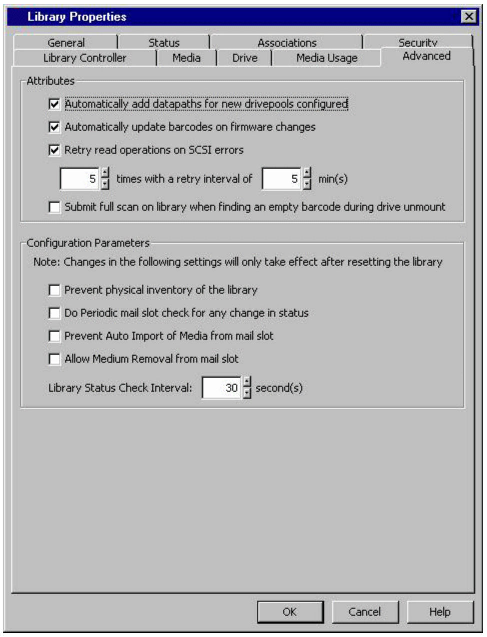
6. Optionally, perform the following steps if you want the system to automatically create the alternate data paths in the Storage Policy Copy that was created during the library configuration.

NOTES

A data path is the combination of MediaAgent, Library, Drive Pool and Scratch Pool used by the storage policy copy to access the library. When you have several MediaAgents accessing a library, you can create a Storage Policy when you configure the library the first time. For subsequent MediaAgents, you can do the following:

- Create alternate data paths in the Storage Policy copies associated with the Storage Policy, using the other MediaAgent, Library, Drive Pool and Scratch Pool combinations.
- Disable the option to automatically create a new storage policy when the library is subsequently configured using another MediaAgent.

- From the CommCell Console, right click the appropriate library and then click **Properties**.
- From the **Library Properties** dialog box, click the **Advanced** tab.
- Enable the **Automatically add datapaths for new drivepools configured** option.



Library Properties

General | Status | Associations | Security | Library Controller | Media | Drive | Media Usage | Advanced

Attributes

☑ Automatically add datapaths for new drivepools configured

☑ Automatically update barcodes on firmware changes

☑ Retry read operations on SCSI errors

5 times with a retry interval of 5 min(s)

☐ Submit full scan on library when finding an empty barcode during drive unmount

Configuration Parameters

Note: Changes in the following settings will only take effect after resetting the library

☐ Prevent physical inventory of the library

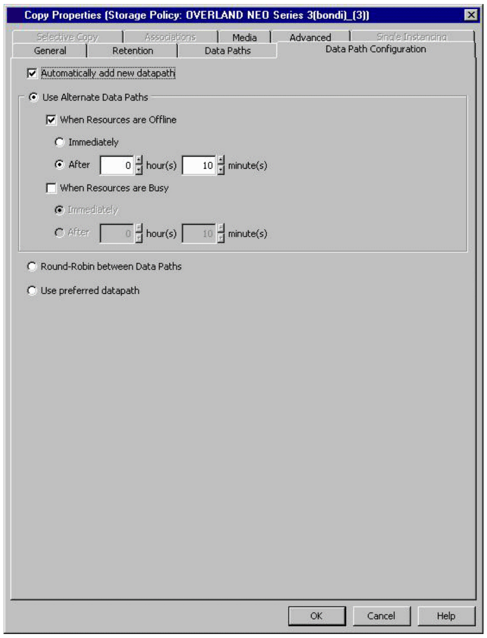
☐ Do Periodic mail slot check for any change in status

☐ Prevent Auto Import of Media from mail slot

☐ Allow Medium Removal from mail slot

Library Status Check Interval: 30 second(s)

- From the CommCell Console, right-click the Storage Policy Copy that was created during the library configuration and then click **Properties**.
- From the **Copy Properties** dialog box, click the **Data Path Configuration** tab.
- Enable the **Automatically add new datapaths** option.



Copy Properties (Storage Policy: OVERLAND NEO Series 3(bondi)_(3))

Selective Copy | Associations | Media | Advanced | Single Instancing | General | Retention | Data Paths | Data Path Configuration

☑ Automatically add new datapath

● Use Alternate Data Paths

☑ When Resources are Offline

○ Immediately

● After 0 hour(s) 10 minute(s)

☐ When Resources are Busy

● Immediately

○ After 0 hour(s) 10 minute(s)

○ Round-Robin between Data Paths

○ Use preferred datapath

TO AUTOMATICALLY CONFIGURE THE OTHER MEDIAAGENTS THAT SHARE THE LIBRARY IN SAN

7. Install the library and ensure that the operating system detects the library. (See Driver Configurations for information on how to check this information for various operating systems.)

8. Install the MediaAgent software on all the other computers that will share the library. (See MediaAgent Deployment for information on installing the MediaAgent software.)

   If you have already installed the MediaAgent software, stop and start the MediaAgent Services on all the MediaAgents sharing this library.

   For more information on stopping and starting services, see the following topics:

   - Stop Services on Windows

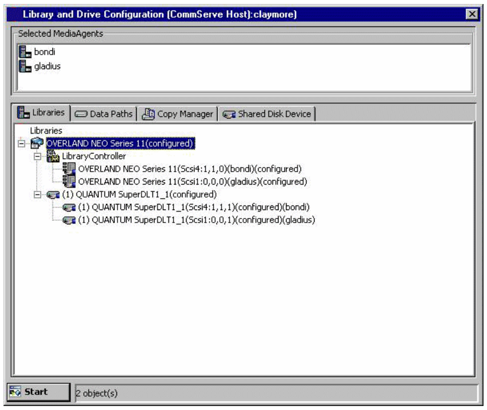
     Start Services on Windows
   - Stop Services on Novell

     Start Services on Novell
   - Stop Services on Unix

     Start Services on Unix

Open the Library and Drive Configuration window and verify that the libraries are configured from all the MediaAgents that share the library.

The **Library** tab provides the physical view of the devices (library and drives).

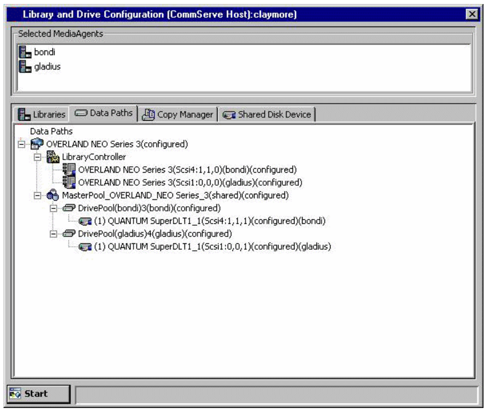


bondi
gladius

```
Libraries
OVERLAND NEO Series 11(configured)
    LibraryController
        OVERLAND NEO Series 11(Scsi4:1,1,0)(bondi)(configured)
        OVERLAND NEO Series 11(Scsi1:0,0,0)(gladius)(configured)
    (1) QUANTUM SuperDLT1_1(configured)
        (1) QUANTUM SuperDLT1_1(Scsi4:1,1,1)(configured)(bondi)
        (1) QUANTUM SuperDLT1_1(Scsi1:0,0,1)(configured)(gladius)
```

2 object(s)

The **Data Paths** tab provides a logical view of the data path used to access the devices - library, master drive pool, drive pool, drive.



bondi
gladius

```
Data Paths
OVERLAND NEO Series 3(configured)
    LibraryController
        OVERLAND NEO Series 3(Scsi4:1,1,0)(bondi)(configured)
        OVERLAND NEO Series 3(Scsi1:0,0,0)(gladius)(configured)
    MasterPool_OVERLAND_NEO Series_3(shared)(configured)
        DrivePool(bondi)3(bondi)(configured)
            (1) QUANTUM SuperDLT1_1(Scsi4:1,1,1)(configured)(bondi)
        DrivePool(gladius)4(gladius)(configured)
            (1) QUANTUM SuperDLT1_1(Scsi1:0,0,1)(configured)(gladius)
```

POST-CONFIGURATION CONSIDERATIONS

After configuring all the libraries, consider disabling the hat the **Auto Configure DDS DrivePool** and **Auto Configure Failover Library Controllers** options described in Step 4, if you do not want the system to automatically configure the library whenever a new MediaAgent is installed in the SAN.

MANUALLY CONFIGURE LIBRARIES SHARED ACROSS A SAN

The following procedure describes the steps involved in configuring a library that is shared across a SAN with DDS, in both the clustered and non-clustered environment. This procedure does not apply to NAS-attached libraries. See Manually Configure NAS-attached Libraries Shared Across a SAN for step-by-step instructions on configuring NAS-attached libraries.

BEFORE YOU BEGIN

Check the following before you configure the library in the SAN environment:

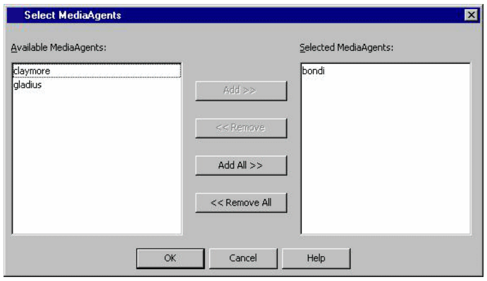
- Hardware is configured according to the conventions detailed in Hardware Configuration Guidelines - Libraries Attached to a SAN.
- MediaAgent software is installed on every computer that is connected to the SAN, and that will access the library. The MediaAgent software can be installed on the computers in any order; the installation sequence does not affect the library configuration.
- Whether the library supports the SCSI 3 drive identification information. To detect whether the library supports SCSI 3, run the **CVScsiTool.exe** available in the `<Software Installation Path>\Base` folder from the command prompt. If SCSI 3 is available, the **Drive Identifiers** will be displayed under **Library Information**. For detailed description of SCSI 3 drive identification, see Detection for libraries that support SCSI 3 drive identification information.
- Note the following for configuring a library attached to the MediaAgent on a cluster:
  - MediaAgent clustering can be supported only for libraries in the SAN environment.
  - Configure the MediaAgents on an active node. The active node takes care of copying the necessary configuration information to the passive nodes.
  - Ensure that both the active and passive nodes are up and running before you begin the configuration.
- This feature requires a Feature License to be available in the CommServe® Server.

  Review general license requirements included in License Administration. Also, View All Licenses provides step-by-step instructions on how to view the license information.

TO MANUALLY CONFIGURE LIBRARIES SHARED ACROSS SAN

1. Display the Library and Drive Configuration window.

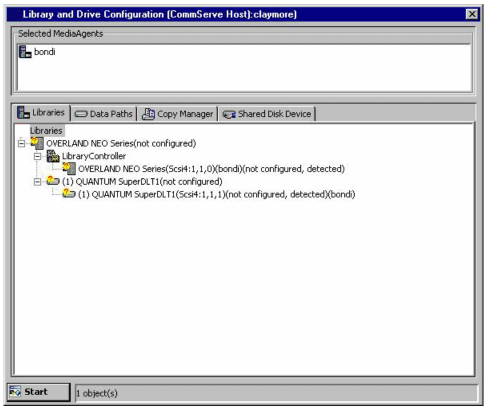
In the **Select MediaAgents** dialog box, select the name of *only one* MediaAgent that will share the library.



2. Detect the devices. Use Detection or Exhaustive Detection as required.

If the library supports SCSI 3 drive identification, it is not necessary to perform an exhaustive detection.

The library and all drives are displayed for the MediaAgent that is connected to the SAN in the **Library and Drive Configuration** window.


Library and Drive Configuration (CommServe Host):claymore)
Selected MediaAgents
bondi
Libraries
Data Paths
Copy Manager
Shared Disk Device
Libraries
OVERLAND NEO Series(not configured)
LibraryController
OVERLAND NEO Series(Scsi4:1,1,0)(bondi)(not configured, detected)
(1) QUANTUM SuperDLT1(not configured)
(1) QUANTUM SuperDLT1(Scsi4:1,1,1)(not configured, detected)(bondi)
Start
1 object(s)

For a Solaris MediaAgent in the SAN environment, the operation will fail to detect devices with SCSI target higher than 15 and/or LUN higher than 7. In a such a situation additional entries must be added for such devices in the **wa.conf** file. For information on adding these entries see Add Additional Entries in **wa.conf** File in the Solaris MediaAgent.

For a NetWare MediaAgent, you may see a number of drives in addition to the drives that are actually present. These drives are displayed as empty slots. You can ignore these empty slots and configure the library using the drives that were detected successfully.

If any additional drives are visible on any of the MediaAgents due to incorrect zoning you must do one of the following:

- Correct the zoning and restart the configuration process.
- Delete the additional drives before performing the next step.

3. Configure the library as described in Configure Devices.

TO AUTOMATICALLY CONFIGURE THE DATA PATHS IN THE STORAGE POLICY COPY

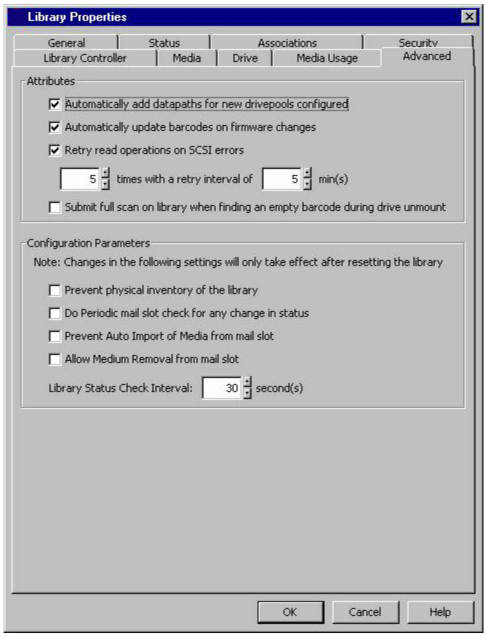
4. Optionally, perform the following steps if you want the system to automatically create the alternate data paths in the Storage Policy Copy that was created during the library configuration.

NOTES

A data path is the combination of MediaAgent, Library, Drive Pool and Scratch Pool used by the storage policy copy to access the library. When you have several MediaAgents accessing a library, you can create a Storage Policy when you configure the library the first time. For subsequent MediaAgents, you can do the following:

- Create alternate data paths in the Storage Policy copies associated with the Storage Policy, using the other MediaAgent, Library, Drive Pool and Scratch Pool combinations.
- Disable the option to automatically create a new storage policy when the library is subsequently configured using another MediaAgent.

- From the CommCell Console, right click the appropriate library and then click **Properties**.
- From the **Library Properties** dialog box, click the **Advanced** tab.
- Enable the **Automatically add datapaths for new drivepools configured** option.



Attributes

☑ Automatically add datapaths for new drivepools configured

☑ Automatically update barcodes on firmware changes

☑ Retry read operations on SCSI errors

5 times with a retry interval of 5 min(s)

☐ Submit full scan on library when finding an empty barcode during drive unmount

Configuration Parameters

Note: Changes in the following settings will only take effect after resetting the library

☐ Prevent physical inventory of the library

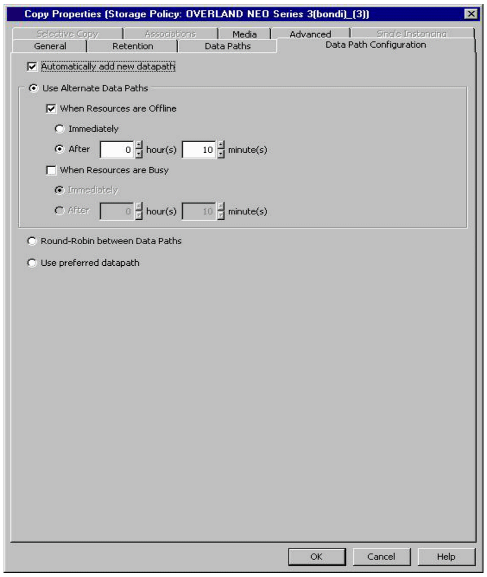
☐ Do Periodic mail slot check for any change in status

☐ Prevent Auto Import of Media from mail slot

☐ Allow Medium Removal from mail slot

Library Status Check Interval: 30 second(s)

- From the CommCell Console, right-click the Storage Policy Copy that was created during the library configuration and then click **Properties**.
- From the **Copy Properties** dialog box, click the **Data Path Configuration** tab.
- Enable the **Automatically add new datapaths** option.



☑ Automatically add new datapath

● Use Alternate Data Paths

☑ When Resources are Offline

○ Immediately

● After 0 hour(s) 10 minute(s)

☐ When Resources are Busy

● Immediately

○ After 0 hour(s) 10 minute(s)

○ Round-Robin between Data Paths

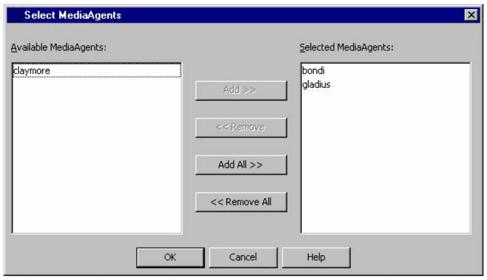
○ Use preferred datapath

TO CONFIGURE THE OTHER MEDIAAGENTS THAT SHARE THE LIBRARY IN SAN

5. From the **Library and Drive Configuration** window, click the **Start** menu and choose **Select MediaAgents**.

   Select the following MediaAgents:

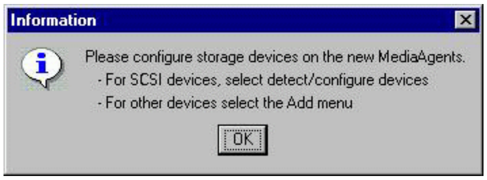
   - The MediaAgent in which the library is already configured.
   - Other MediaAgent(s) in which you wish to configure the library using DDS.



Available MediaAgents: claymore

Selected MediaAgents: bondi, gladius

6. Click **OK** in the **Information** prompt.



Please configure storage devices on the new MediaAgents.
- For SCSI devices, select detect/configure devices
- For other devices select the Add menu

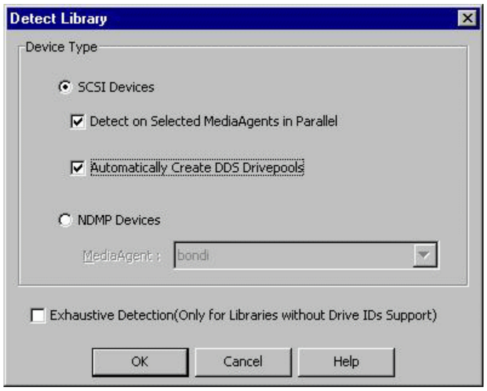
7. Detect the devices that are controlled by MediaAgents that will access the library as described in Detect Devices.

   In the **Detect Library** dialog box, select the following options:

   - **Detect on Selected MediaAgents in Parallel**
   - **Automatically create DDS Drivepools**

   NOTES

   - The option to automatically create/configure DDS DrivePools is not available for NAS-attached libraries; Dynamic Drive Sharing must be configured manually. For instructions on how to configure DDS for NAS-attached libraries, see Configure NAS-attached Libraries Shared Across a SAN .



Detect Library

Device Type

● SCSI Devices

☑ Detect on Selected MediaAgents in Parallel

☑ Automatically Create DDS Drivepools

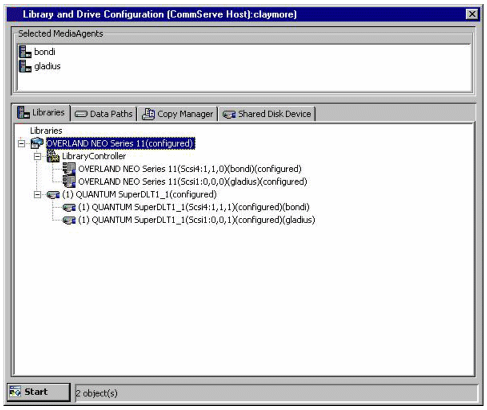
○ NDMP Devices

MediaAgent : bondi

□ Exhaustive Detection(Only for Libraries without Drive IDs Support)

The system detects the drives and automatically displays them with the DDS setup in the **Library and Drive Configuration** window.

The **Library** tab provides the physical view of the devices (library and drives).



Library and Drive Configuration (CommServe Host):claymore)

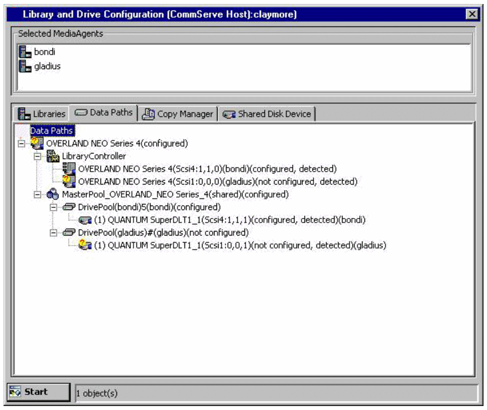
Selected MediaAgents

bondi
gladius

```
Libraries
OVERLAND NEO Series 11(configured)
  LibraryController
    OVERLAND NEO Series 11(Scsi4:1,1,0)(bondi)(configured)
    OVERLAND NEO Series 11(Scsi1:0,0,0)(gladius)(configured)
  (1) QUANTUM SuperDLT1_1(configured)
    (1) QUANTUM SuperDLT1_1(Scsi4:1,1,1)(configured)(bondi)
    (1) QUANTUM SuperDLT1_1(Scsi1:0,0,1)(configured)(gladius)
```

2 object(s)

The **Data Paths** tab provides a logical view of the data path used to access the devices - library, master drive pool, drive pool, drive.



Library and Drive Configuration (CommServe Host):claymore)

Selected MediaAgents

bondi
gladius

```
Data Paths
OVERLAND NEO Series 4(configured)
  LibraryController
    OVERLAND NEO Series 4(Scsi4:1,1,0)(bondi)(configured, detected)
    OVERLAND NEO Series 4(Scsi1:0,0,0)(gladius)(not configured, detected)
  MasterPool_OVERLAND_NEO Series_4(shared)(configured)
    DrivePool(bondi)5(bondi)(configured)
      (1) QUANTUM SuperDLT1_1(Scsi4:1,1,1)(configured, detected)(bondi)
    DrivePool(gladius)#(gladius)(not configured)
      (1) QUANTUM SuperDLT1_1(Scsi1:0,0,1)(not configured, detected)(gladius)
```

1 object(s)

8. Configure the library as described in Configure Devices.

   This will configure the library and the library controllers for the library.

   If you do not wish to configure the library controllers on one or more of the MediaAgents, you must delete them before configuring the library.

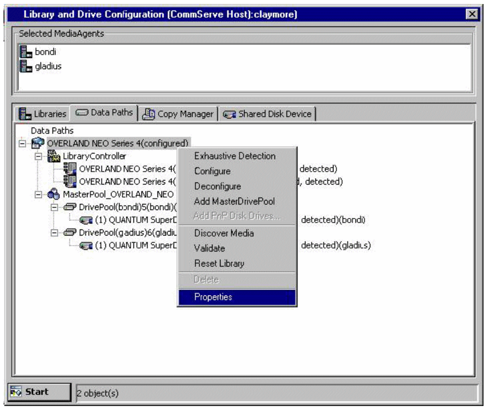
   To delete, right-click the appropriate library controller and then choose **Delete**. Click **OK** in the confirmation prompt that appears.

POST CONFIGURATION CONSIDERATIONS

If you subsequently add new MediaAgents with visibility to a configured library and drives, the system will automatically configure the libraries and drives in those MediaAgents.

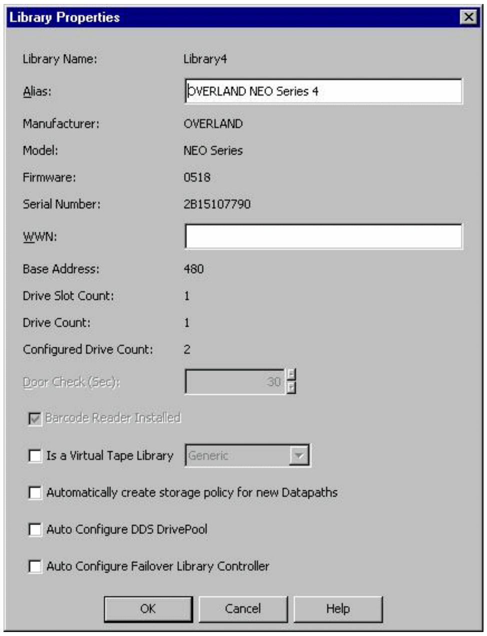
Perform the following steps if you wish to disable the automatic library and drive configuration in such MediaAgents:

From the **Library and Drive Configuration** window, open the **Library Properties** dialog box associated with the library you wish to disable automatic configuration.



Disable the following options:

- Auto Configure DDS DrivePool
- Auto Configure Failover Library Controller


Library Properties

Library Name: Library4

Alias: OVERLAND NEO Series 4

Manufacturer: OVERLAND

Model: NEO Series

Firmware: 0518

Serial Number: 2B15107790

WWN:

Base Address: 480

Drive Slot Count: 1

Drive Count: 1

Configured Drive Count: 2

Door Check (Sec): 30

☑ Barcode Reader Installed

☐ Is a Virtual Tape Library Generic

☐ Automatically create storage policy for new Datapaths

☐ Auto Configure DDS DrivePool

☐ Auto Configure Failover Library Controller

Configure NAS-attached Libraries Shared Across a SAN

The following procedure explains the steps involved in configuring a NAS-attached library which is shared in the SAN environment by multiple NAS file servers and/or MediaAgents.

BEFORE YOU BEGIN

- During configuration, all of the drive devices must have a value for their serial number. If the automatic configuration does not populate a serial number for a drive, you must manually enter a serial number value, using the Manually configure the library and drives attached to the NAS file server procedure. Each instance of a drive must have the same serial number.
- During configuration of NAS-attached libraries and drives, connectivity is required between the CommServe and the NAS file server. Even after configuration is complete, connectivity is still required to the CommServe for various operations, such as cleaning up snapshots from a killed NAS *i*DataAgent job.
- This feature requires a Feature License to be available in the CommServe® Server.

  Review general license requirements included in License Administration. Also, View All Licenses provides step-by-step instructions on how to view the license information.

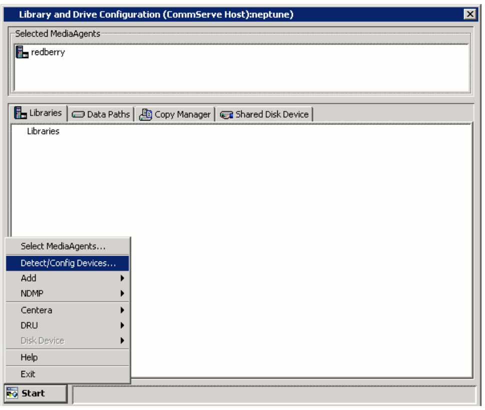
CONFIGURATION PROCEDURE

1. You must first configure the library from any one of the MediaAgents that share the library across a SAN. Use one of the following procedures to configure the library for the first time:
   - If you wish to configure the library using a NAS file server first - see Configure a library and drives attached to the NAS file server using automatic detection for step-by-step instructions.
   - If you wish to configure the library using a MediaAgent first - see Automatically Configure Libraries Shared Across a SAN for step-by-step instructions.

Once you have configured the library for the first time you can use the following procedure to configure the library from a NAS file server.

2. Display the Library and Drive Configuration window.
3. If necessary, select a new MediaAgent that must be used by the File Server to communicate.

   To select a new MediaAgent, click the **Start** button and then click **Select MediaAgents**. Select the appropriate MediaAgent from the **Select MediaAgent** dialog box and click **OK**.
4. Click the **Start** button, and then select **Detect/Configure Devices**.



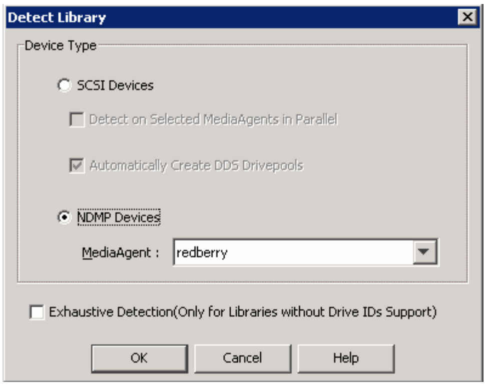
5. Select the **NDMP Devices** and the **MediaAgent** that will control the library.

   Select the **Exhaustive Detection** option.

   Click **OK**.

   NOTES

   - 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.
   - For cluster, select the cluster virtual server as the MediaAgent.


Detect Library

Device Type

○ SCSI Devices

☐ Detect on Selected MediaAgents in Parallel

☑ Automatically Create DDS Drivepools

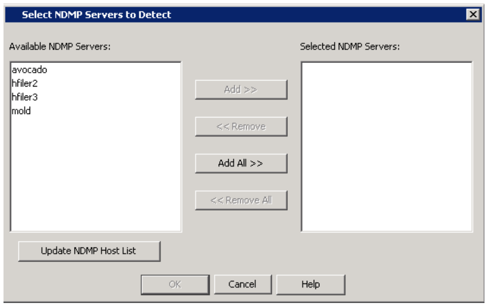
● NDMP Devices

MediaAgent : redberry

☐ Exhaustive Detection(Only for Libraries without Drive IDs Support)

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

   Click **Yes**.
7. Select the File Server from which you wish to detect the library and click **OK**.


Select NDMP Servers to Detect

Available NDMP Servers:

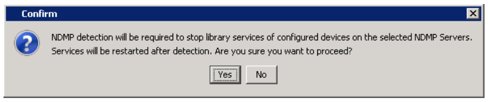
avocado
hfiler2
hfiler3
mold

Selected NDMP Servers:

8. Click **Yes** to start the device detection process.

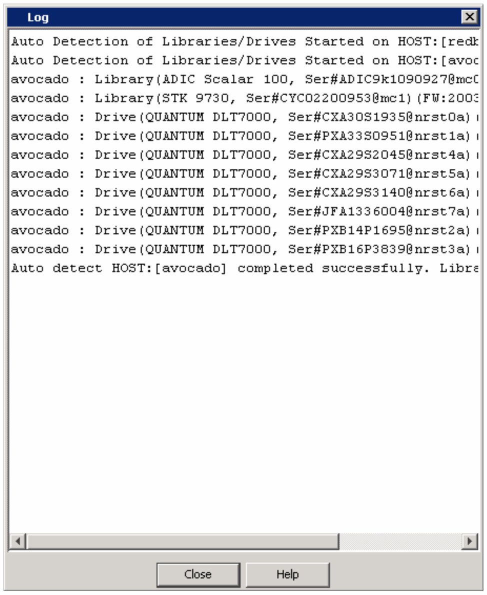
   NOTES

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


Confirm

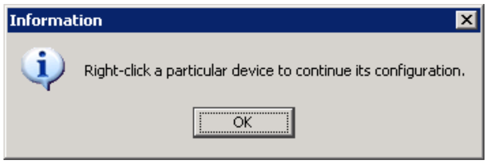
NDMP detection will be required to stop library services of configured devices on the selected NDMP Servers. Services will be restarted after detection. Are you sure you want to proceed?

9. When the exhaustive detection process is completed, the log file is displayed. Note the log file contents and click **Close** to proceed.



```
Auto Detection of Libraries/Drives Started on HOST:[redk
Auto Detection of Libraries/Drives Started on HOST:[avoc
avocado : Library(ADIC Scalar 100, Ser#ADIC9k1090927@mc0
avocado : Library(STK 9730, Ser#CYC02200953@mc1)(FW:2003
avocado : Drive(QUANTUM DLT7000, Ser#CXA30S1935@nrst0a)
avocado : Drive(QUANTUM DLT7000, Ser#PXA33S0951@nrst1a)
avocado : Drive(QUANTUM DLT7000, Ser#CXA29S2045@nrst4a)
avocado : Drive(QUANTUM DLT7000, Ser#CXA29S3071@nrst5a)
avocado : Drive(QUANTUM DLT7000, Ser#CXA29S3140@nrst6a)
avocado : Drive(QUANTUM DLT7000, Ser#JFA1336004@nrst7a)
avocado : Drive(QUANTUM DLT7000, Ser#PXB14P1695@nrst2a)
avocado : Drive(QUANTUM DLT7000, Ser#PXB16P3839@nrst3a)
Auto detect HOST:[avocado] completed successfully. Libra
```

10. An **Information** prompt appears, informing you to right-click the device to continue the configuration. Click **OK** to proceed



Right-click a particular device to continue its configuration.

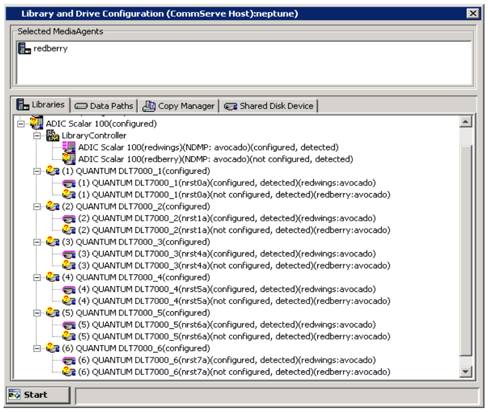
11. When the Exhaustive Detection is completed, the system displays the devices in the **Library and Drive Configuration** window.

NOTES

- New detected devices are not configured at this point, and the configuration information will not be saved when you exit from the **Library and Drive Configuration** window until those devices are configured.

Right-click the library and then click **Configure**.

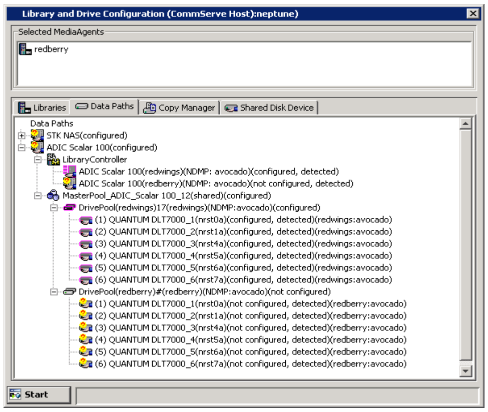
The **Library** tab provides the physical view of the devices (library and drives).



redberry

```
ADIC Scalar 100(configured)
    LibraryController
        ADIC Scalar 100(redwings)(NDMP: avocado)(configured, detected)
        ADIC Scalar 100(redberry)(NDMP: avocado)(not configured, detected)
    (1) QUANTUM DLT7000_1(configured)
        (1) QUANTUM DLT7000_1(nrst0a)(configured, detected)(redwings:avocado)
        (1) QUANTUM DLT7000_1(nrst0a)(not configured, detected)(redberry:avocado)
    (2) QUANTUM DLT7000_2(configured)
        (2) QUANTUM DLT7000_2(nrst1a)(configured, detected)(redwings:avocado)
        (2) QUANTUM DLT7000_2(nrst1a)(not configured, detected)(redberry:avocado)
    (3) QUANTUM DLT7000_3(configured)
        (3) QUANTUM DLT7000_3(nrst4a)(configured, detected)(redwings:avocado)
        (3) QUANTUM DLT7000_3(nrst4a)(not configured, detected)(redberry:avocado)
    (4) QUANTUM DLT7000_4(configured)
        (4) QUANTUM DLT7000_4(nrst5a)(configured, detected)(redwings:avocado)
        (4) QUANTUM DLT7000_4(nrst5a)(not configured, detected)(redberry:avocado)
    (5) QUANTUM DLT7000_5(configured)
        (5) QUANTUM DLT7000_5(nrst6a)(configured, detected)(redwings:avocado)
        (5) QUANTUM DLT7000_5(nrst6a)(not configured, detected)(redberry:avocado)
    (6) QUANTUM DLT7000_6(configured)
        (6) QUANTUM DLT7000_6(nrst7a)(configured, detected)(redwings:avocado)
        (6) QUANTUM DLT7000_6(nrst7a)(not configured, detected)(redberry:avocado)
```

The **Data Paths** tab provides a logical view of the data path used to access the devices - library, master drive pool, drive pool, drive.



redberry

```
Data Paths
STK NAS(configured)
ADIC Scalar 100(configured)
    LibraryController
        ADIC Scalar 100(redwings)(NDMP: avocado)(configured, detected)
        ADIC Scalar 100(redberry)(NDMP: avocado)(not configured, detected)
    MasterPool_ADIC_Scalar 100_12(shared)(configured)
        DrivePool(redwings)17(redwings)(NDMP:avocado)(configured)
            (1) QUANTUM DLT7000_1(nrst0a)(configured, detected)(redwings:avocado)
            (2) QUANTUM DLT7000_2(nrst1a)(configured, detected)(redwings:avocado)
            (3) QUANTUM DLT7000_3(nrst4a)(configured, detected)(redwings:avocado)
            (4) QUANTUM DLT7000_4(nrst5a)(configured, detected)(redwings:avocado)
            (5) QUANTUM DLT7000_5(nrst6a)(configured, detected)(redwings:avocado)
            (6) QUANTUM DLT7000_6(nrst7a)(configured, detected)(redwings:avocado)
        DrivePool(redberry)#(redberry)(NDMP:avocado)(not configured)
            (1) QUANTUM DLT7000_1(nrst0a)(not configured, detected)(redberry:avocado)
            (2) QUANTUM DLT7000_2(nrst1a)(not configured, detected)(redberry:avocado)
            (3) QUANTUM DLT7000_3(nrst4a)(not configured, detected)(redberry:avocado)
            (4) QUANTUM DLT7000_4(nrst5a)(not configured, detected)(redberry:avocado)
            (5) QUANTUM DLT7000_5(nrst6a)(not configured, detected)(redberry:avocado)
            (6) QUANTUM DLT7000_6(nrst7a)(not configured, detected)(redberry:avocado)
```

12. Configure the library as described in Configure Devices.

13. If you have configured the library, the status of the library changes to configured.

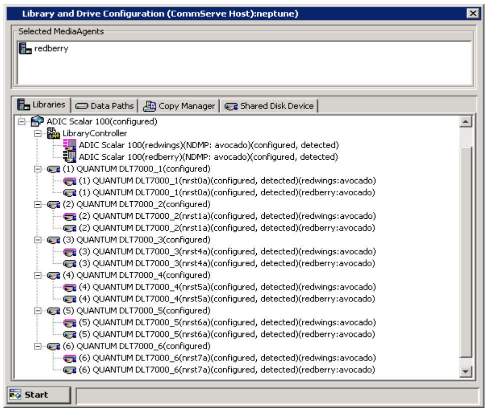
If you chose to configure all associated drives, the status of the drives, the master drive pool, and drive pool that contains the drives changes to configured.

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

NOTES

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

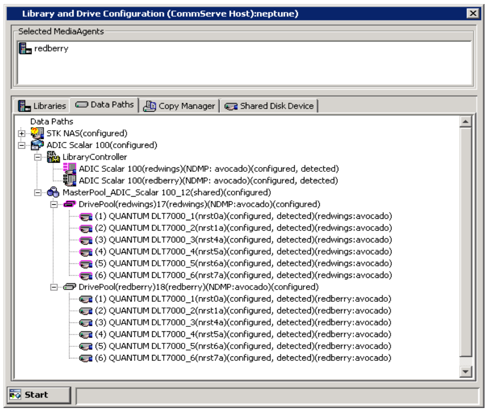
The **Library** tab provides the physical view of the devices (library and drives).



```
ADIC Scalar 100(configured)
    LibraryController
        ADIC Scalar 100(redwings)(NDMP: avocado)(configured, detected)
        ADIC Scalar 100(redberry)(NDMP: avocado)(configured, detected)
    (1) QUANTUM DLT7000_1(configured)
        (1) QUANTUM DLT7000_1(nrst0a)(configured, detected)(redwings:avocado)
        (1) QUANTUM DLT7000_1(nrst0a)(configured, detected)(redberry:avocado)
    (2) QUANTUM DLT7000_2(configured)
        (2) QUANTUM DLT7000_2(nrst1a)(configured, detected)(redwings:avocado)
        (2) QUANTUM DLT7000_2(nrst1a)(configured, detected)(redberry:avocado)
    (3) QUANTUM DLT7000_3(configured)
        (3) QUANTUM DLT7000_3(nrst4a)(configured, detected)(redwings:avocado)
        (3) QUANTUM DLT7000_3(nrst4a)(configured, detected)(redberry:avocado)
    (4) QUANTUM DLT7000_4(configured)
        (4) QUANTUM DLT7000_4(nrst5a)(configured, detected)(redwings:avocado)
        (4) QUANTUM DLT7000_4(nrst5a)(configured, detected)(redberry:avocado)
    (5) QUANTUM DLT7000_5(configured)
        (5) QUANTUM DLT7000_5(nrst6a)(configured, detected)(redwings:avocado)
        (5) QUANTUM DLT7000_5(nrst6a)(configured, detected)(redberry:avocado)
    (6) QUANTUM DLT7000_6(configured)
        (6) QUANTUM DLT7000_6(nrst7a)(configured, detected)(redwings:avocado)
        (6) QUANTUM DLT7000_6(nrst7a)(configured, detected)(redberry:avocado)
```

The **Data Paths** tab provides a logical view of the data path used to access the devices - library, master drive pool, drive pool, drive.

This task is now complete.



```
Data Paths
STK NAS(configured)
ADIC Scalar 100(configured)
    LibraryController
        ADIC Scalar 100(redwings)(NDMP: avocado)(configured, detected)
        ADIC Scalar 100(redberry)(NDMP: avocado)(configured, detected)
    MasterPool_ADIC_Scalar 100_12(shared)(configured)
        DrivePool(redwings)17(redwings)(NDMP:avocado)(configured)
            (1) QUANTUM DLT7000_1(nrst0a)(configured, detected)(redwings:avocado)
            (2) QUANTUM DLT7000_2(nrst1a)(configured, detected)(redwings:avocado)
            (3) QUANTUM DLT7000_3(nrst4a)(configured, detected)(redwings:avocado)
            (4) QUANTUM DLT7000_4(nrst5a)(configured, detected)(redwings:avocado)
            (5) QUANTUM DLT7000_5(nrst6a)(configured, detected)(redwings:avocado)
            (6) QUANTUM DLT7000_6(nrst7a)(configured, detected)(redwings:avocado)
        DrivePool(redberry)18(redberry)(NDMP:avocado)(configured)
            (1) QUANTUM DLT7000_1(nrst0a)(configured, detected)(redberry:avocado)
            (2) QUANTUM DLT7000_2(nrst1a)(configured, detected)(redberry:avocado)
            (3) QUANTUM DLT7000_3(nrst4a)(configured, detected)(redberry:avocado)
            (4) QUANTUM DLT7000_4(nrst5a)(configured, detected)(redberry:avocado)
            (5) QUANTUM DLT7000_5(nrst6a)(configured, detected)(redberry:avocado)
            (6) QUANTUM DLT7000_6(nrst7a)(configured, detected)(redberry:avocado)
```

Configure a Library with Mixed Drive Types in SAN

The following sections provide guidelines on configuring a library with mixed drive types in the SAN environment. (This procedure does not apply to NAS-attached libraries.)

CONSIDERATIONS FOR A LIBRARY WITH MIXED DRIVE TYPES IN SAN

1. Configure any of the MediaAgents sharing the library as described in Configure a Library with Mixed Drive Types.
2. After configuring the library: Display the Library and Drive Configuration window.
3. Open the **Library Properties** dialog box and select the following option:

   - **Auto Configure DDS DrivePool:** Enable this option to automatically configure the DDS drive pools for MediaAgents sharing these drives.

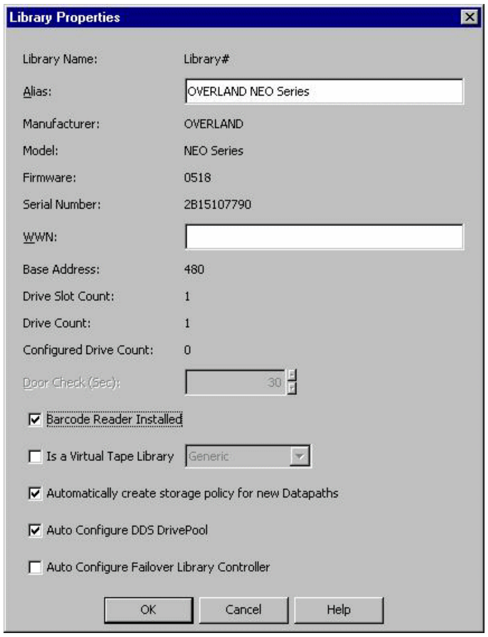
   Optionally, consider the following options:

   - **Auto Configure Failover Library Controllers**: Enable this option to automatically configure the Failover Library Controllers in all the MediaAgents sharing this library.
   - **Automatically create storage policy for new Datapaths**: Disable this option for libraries with mixed drive types.

   Click **OK**.

   NOTES

   - The option to automatically create/configure DDS DrivePools is not available for NAS-attached libraries; Dynamic Drive Sharing must be configured manually. For instructions on how to configure DDS for NAS-attached libraries, see Configure NAS-attached Libraries Shared Across a SAN .



Library Name:	Library#
Alias:	OVERLAND NEO Series
Manufacturer:	OVERLAND
Model:	NEO Series
Firmware:	0518
Serial Number:	2B15107790
WWN:	
Base Address:	480
Drive Slot Count:	1
Drive Count:	1
Configured Drive Count:	0
Door Check (Sec):	30

☑ Barcode Reader Installed

☐ Is a Virtual Tape Library Generic

☑ Automatically create storage policy for new Datapaths

☑ Auto Configure DDS DrivePool

☐ Auto Configure Failover Library Controller

TO AUTOMATICALLY CONFIGURE THE OTHER MEDIAAGENTS THAT SHARE THE LIBRARY IN SAN

4. Install the library and ensure that the operating system detects the library. (See Driver Configurations for information on how to check this information for various operating systems.)

5. Install the MediaAgent software on all the other computers that will share the library. (See MediaAgent Deployment for information on installing the MediaAgent software.)

   If you have already installed the MediaAgent software, stop and start the MediaAgent Services on all the MediaAgents sharing this library.

   For more information on stopping and starting services, see the following topics:

   - Stop Services on Windows

     Start Services on Windows
   - Stop Services on Novell

     Start Services on Novell
   - Stop Services on Unix

     Start Services on Unix

   Open the Library and Drive Configuration window and verify that the libraries are configured from all the MediaAgents that share the library.

POST CONFIGURATION CONSIDERATIONS

Consider the following:

- When you create new storage policies, or have existing storage policies, ensure that the appropriate combination of drive pool and scratch pool are associated with them.
- Also when you configure the alternate data paths in a storage policy copy, ensure that the same combination of drive pool and scratch pool are added as the alternate paths .

SAN-Attached Libraries - How To

Topics | Best Practices | Configure | How To | Troubleshoot | Related Topics

Add Additional Entries in wa.conf File in the Solaris MediaAgent

Manually Switch Active Library Controllers

View the Status of the Library Controller

ADD ADDITIONAL ENTRIES IN WA.CONF FILE IN THE SOLARIS MEDIAAGENT

To add additional entries in wa.conf file in Solaris MediaAgent:

1. Make sure devices are connected properly and appropriate drivers are installed.
2. Stop the services on the MediaAgent in which you wish to add the entries.
3. Open the following file to find the devices with SCSI target higher than 15 and/or LUN higher than 7.

   ```
   /var/adm/messages
   ```
4. Add the necessary entries in the following file:

   ```
   /usr/kernel/drv/wa.conf
   ```

   Use the following pattern to add each device:

   ```
   name="wa" class="scsi" target="target number of the device"

   lun="lun number of the devices";
   ```
5. Save the changes.
6. Execute the following commands to create the device nodes:

   ```
   rem_drv wa

   add_drv wa
   ```
7. Start the services in the MediaAgent in which the entries were added.

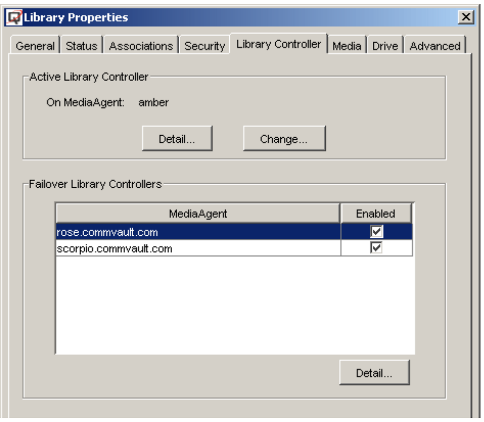
MANUALLY SWITCH THE ACTIVE LIBRARY CONTROLLER

BEFORE YOU BEGIN

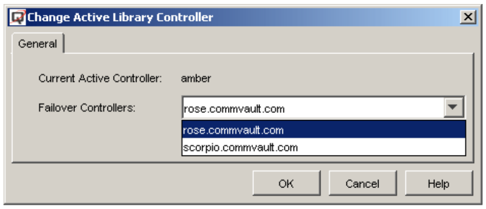
Do not switch the active library controller if jobs are in progress for that MediaAgent.

TO MANUALLY SWITCH AN ACTIVE LIBRARY CONTROLLER

1. From the CommCell Console, right-click the library for which you wish to switch the active library controller, and then click **Properties**.
2. Click the **Library Controller** tab in the **Library Properties** dialog box.



3. Click **Change**.
4. In the **Change Active Library Controller** dialog box, choose the library controller that you wish to designate as the active library controller from the **Failover Controller** list.



In order to manually change a failover library controller candidate as the active library controller, the failover library controller candidate must be **Alive** and **Enabled**.

5. Click **OK** in both the **Change Active Library Controller** dialog box and in the **Library Properties** dialog box.
6. The selected failover library controller is switched as the active library controller.

VIEW THE STATUS OF THE LIBRARY CONTROLLER

Required Capability: See Capabilities and Permitted Actions

To view the status of the library controller:

1. From the CommCell Browser, right-click the library for which you wish to view the library controller status, and then click **Properties**.
2. Click the Library Controller tab.

   The status of the library controller can be viewed in the **Library Properties (Library Controller)** dialog box. Note the following:

   The **Active Library Controller** is the MediaAgent with the **Active**, **Alive** and **Enabled** status as *YES*, and the **Soft State** as *ON*. (You can view the status of the library controllers by clicking the **Detail** button on the **Active Library Controller** or **Failover Library Controller** panes.)

   - In a library configured in the SAN environment, where several MediaAgents are configured as library controllers, at any given point, the MediaAgent accessing the library is considered as **Active** and therefore displayed as the Active Library Controller. All the other MediaAgents are displayed as **Failover Library Controllers**. The **Active** status will be displayed as *No* for the failover library controllers.
   - In a library configured in the non-SAN environment, where only one MediaAgent is configured as a library controller, the MediaAgent is displayed as the Active Library Controller. If either the Alive or Enabled status is NO, or Soft State is OFF, the Active status will be displayed as OFF and the MediaAgent will be displayed as a **Failover Library Controller**.

Stand-Alone Drives

Topics | Configure | How to | Troubleshoot | Related Topics

OVERVIEW

A stand-alone library is a one-drive storage unit with no media storage capability, no media changer, and no barcode reader.

> As stand-alone drives do not have the facility to store used media, it is your responsibility to label and store all used media in a secure and accessible location.

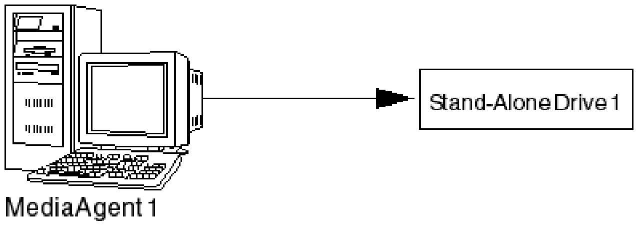
Removable Disk Drives are also configured as a stand-alone library.

All the features described in following sections apply to both stand-alone drives and removable disk drives unless otherwise stated.

CONFIGURING STAND-ALONE DRIVES

SINGLE LIBRARY CONFIGURATION

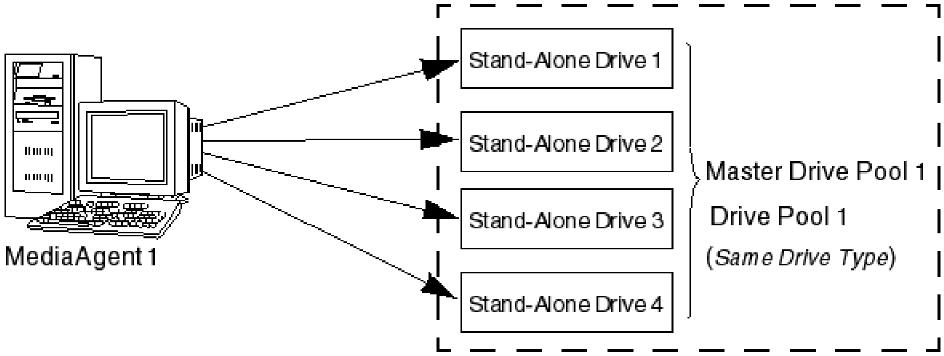
The stand-alone drive is physically attached to the MediaAgent that controls the library as represented in the following illustration:



Configure a Stand-Alone Drive provides step-by-step instructions on how to configure such a library.

DRIVE POOLING STAND-ALONE DRIVES

Several stand-alone drives with the same drive type are attached to a MediaAgent. These stand-alone drives can be pooled together as a Drive Pool. This is represented in the following illustration:



Drive pooling offers the following advantages:

- **Automatic Tape spanning for large data protection operations**

  When performing large data protection operations, the operation will automatically span to another media in another drive when the currently active media is full, without any manual user intervention.

- **Facility to perform multi-streamed data protection jobs**

  Multiple streams provide the means to parallelize an operation and thus improve the rate at which data can be written to or retrieved from the storage media. As each stream requires a drive and a storage media, drive pooling provides the facility to run multi-streamed data protection operations.

Configure Multiple Stand-Alone Drives into a Drive Pool provides step-by-step instructions on how to configure several stand-alone drives into a drive pool.

Drive Pooling Stand-Alone Drives That Were Previously Configured as Separate Stand-Alone Drives provides step-by-step instructions on how to re-configure existing stand-alone drives (that are not drive pooled) into a drive pool.

MEDIA LABELING IN STAND-ALONE DRIVES

AUTOMATIC LABELING SCHEMES

Facility to automate the process of labeling media (On Media Label - OML) associated with stand-alone drives is provided. Several Label Options are provided to suit the labeling conventions used in your organization.

Care must be exercised while generating the labeling scheme to ensure that each media label is unique. If the specified labeling scheme is not unique, and if duplicate labels are found, the system automatically appends a media ID to make it unique.

The following list provides some examples of labeling schemes:

- If a separate media is used for each day of the week and if every month a new set of media is used, the following labeling format can be used:

  <DAY>_<DATE>

  This would generate a label as follows on each of the media associated with each day of the week, the first time the media is used in the library:

  Monday_Sep 22 2004, Tuesday_Sep 23 2004, etc.

  The <DAY> would make the label easily identifiable, and the <DATE> in addition to providing the month in the label, also makes the label unique.

- If the media must be identified based on the stand-alone drive in which the media is used, the following labeling format can be used:

  <DRIVE><NUMBERSTART>

  This would generate the following labels:

  BRANCH A 1 (assuming that the drive is named as Branch A)

  If stand-alone drives are pooled together the drive pool name can be used instead of the drive name.

SETTING-UP AUTOMATIC LABELING SCHEMES

Use the following steps to setup the media labeling scheme in stand-alone libraries:

1. Specify the labeling scheme for a stand-alone drive, from the appropriate **Library Properties (Media)** tab. (See Create Automatic Labeling Schemes for step-by-step instructions.)
2. The labels are stamped whenever non-stamped media is found when the system checks the media in the drive to update the media information. See Detecting Media Changes in Stand-Alone Drives for more information.
3. When you introduce a media into the stand-alone drive, you can wait until the system checks for the media in the drive to automatically label them using

the labeling scheme (as explained above) or you can manually stamp the media using either the established labeling scheme or a new label for the media. (See Add Media Identifiers (Stamp Media) for step-by-step instructions.

MANUAL STAMPING OF MEDIA

For PnP libraries, Manual Stamping of Media is supported for libraries that have only one USB drive. It is not supported for PnP libraries that have multiple USB drives.

If the automatic labeling scheme is not established the stamp media operation can be used to pre-label stand-alone tapes, so that it can be introduced as a spare at any time.

We recommend that you affix an external label on the media, with the same unique identifier. This will help you to properly manage the media associated with stand-alone drives

Once stamped, the media can be used in any CommCell that contains a stand-alone drive if the option to overwrite media **When it is from a different CommCell** is enabled from the Media tab of the **Library Properties** dialog box.

Media that are not stamped (either automatically or manually) will be displayed as **Unidentified Media**. Data write operations will use the media, but will create a default system generated OML for the media using the media creation date and time. For example, `StdAln_Wed Nov 10 2004 19:52:38_3`.

Media from another CommCell will also be displayed as **Unidentified Media**. Such media will be overwritten only when the **Overwrite Media - When it is from a different CommCell** option is enabled in the associated **Library Properties (Media)** dialog box.

MEDIA OPERATIONS IN STAND-ALONE DRIVES

Stand-alone libraries do not have an initial list of spare media. The system prompts you to insert a new media whenever it is required. If you have not created the On Media Label using the Automatic Labeling Scheme or the Manual Stamp Media operation, the system creates a default OML for the media, the first time you perform a write operation on the media. Subsequently, if necessary, you can provide your own label for the media at any time. The On Media Label is used to correctly identify the media during subsequent media operations.

When you perform a data write operation using a stand-alone drive:

- If the correct media is available in the drive, the data protection operation will continue.
- If there is no usable media in the drive at the time the job runs, the system would create a temporary dummy media for reservation purposes, and remove it as the actual media becomes available.
- If a new media is inserted, the previously active media is marked as **Appendable** and if a label is not found in the new media, the system writes a default OML and continues with the operation.
- If a recycled media is inserted the previously active media will be marked as **Appendable** and the data protection operation will continue.
- If a media inserted is associated with a different storage policy/copy/stream than that of the current job, you will be prompted to insert the active media or a new or appendable media in the stand-alone drive. The data protection operation will not continue until the correct or new/appendable media is inserted.
- If no media is inserted in the drive, a pop-up window prompts for the required/new media. The pop-up window will be refreshed every three minutes, until the required media is inserted.

  If an operator is not available to insert the required media, we recommend that you avoid scheduling jobs that use different storage policies for a stand-alone drive. If you want to schedule jobs for a stand-alone drive, make sure that all of the jobs use the same storage policy. If a scheduled job uses a different storage policy from the one to which the media in the drive belongs, the job cannot start until someone removes that media and inserts another. This may defeat the purpose of scheduling the job.

- If a spare media is not available, and if another media is available in the stand-alone drive, the system will overwrite the media if it is from the same storage policy and if the **Overwrite Media if Media Last Written to in (n) Days/Hours** option is enabled in the **Library Properties** dialog box associated with the stand-alone drive. This option also allows you to specify the time (in days or hours) after which the media can be over written. This ensures that data protection operations complete successfully, when a spare media or media marked as **Appendable** is not available in the drive. Note, that this option is only applicable for data protection operations, and does not apply for Synthetic Full, Auxiliary Copy and ER backup operations.

  Care must be exercised while enabling this option, as the system will age (prune) and overwrite the data available in the media, if the data is found to be from the same storage policy from which the job is initiated.

- The system will automatically unload the media from the drive when a different media is required when the **Overwrite Media in drive if Media Not Written to in (n) Days/Hours** option is enabled is enabled in the **Library Properties** dialog box associated with the stand-alone drive.

  (If the stand-alone drive supports the automatic ejection of the media from the drive, the media will also be ejected.)

  If this option is not selected, the system will not unload the media from the drive and will overwrite the media (when a job is initiated) if the **Overwrite Media in drive if Media Not Written to in (n) Days/Hours option** is enabled, after the time specified in this option. (See Enable (or Disable) Unloading of Media from a Stand-alone Drive when Different Media is Required for step-by-step instructions.)

All media available in a stand-alone drive are displayed in the CommCell Browser under the **Exported Media** pool. Assigned media will be displayed in the

Assigned Media pool, bad media will be displayed under **Retired Media** and recycled media in the **Default Scratch Pool.**

The system will not unmount the media from the drive once the operation on the media is completed. The media will be displayed in the CommCell Console as mounted in the drive. You can however, unmount the media from the drive after data protection, data recovery and Auxiliary copy operations by enabling the **Unmount Media from the drive after (n) Minutes/Hours of inactivity** option in the **Media Usage** tab of the **Library Properties** dialog box. (See Modify the Unmount Time for Inactive Media in the Drive for step-by-step instructions.)

Pop-up Messages in Stand-Alone Drives

Pop-up messages are displayed for stand-alone drives when a wrong media or no media is available in the drive. These messages are displayed in the following computers:

- MediaAgent computer to which the stand-alone drive is attached
- All machines that have the CommCell Console (stand-alone application) open, when the option **Show Media related Pop up Message in CommCell Console** is enabled in the **Media** tab of the **Library Properties** dialog box.

  See Enable (or Disable) Media Related Pop-Ups in the CommCell Console for step-by-step instructions.

For example, on the MediaAgent machine, if the stand-alone version of the CommCell Console is open, you will see two pop-up messages. You can click the **OK** button in any one of these messages. However, only a response on the MediaAgent computer will take effect. If however, you do not respond to the message, the message is displayed for three minutes and after three minutes the message is automatically refreshed.

> If you click the **Cancel** option in the pop-up message for media request from a data protection or data recovery operation, the mount operation for the media will fail and the job will go to pending or may fail depending on the **Job Restart** options established in the **Advanced** tab of the **Job Management** dialog box. (See Job Preemption Control for more information.)

Detecting Media Changes in Stand-Alone Drives

When the media in a stand-alone drive is removed or changed, the corresponding media information in the CommCell Console can be updated as follows:

- Set up the Automatic Checking of Media in Stand-Alone Drives. This option can be established from the **Drive** tab of the **Library Properties** dialog box. (See Setup Automatic Checking of Media for step-by-step instructions.) When established this option automatically checks the media in the stand-alone drive and updates the information in the CommCell Console. This option also provides the facility to establish, how often this check must be performed to update the information. It is recommended that this option be enabled with frequent updates, so that the media information in the CommCell Console is up-to-date.
- Perform a Verify Media Operation. To manually verify the media in the drive perform a **Verify Media** Operation. This will immediately update the media information in the CommCell Console.

If the Automatic check for media option is not established and if a verify media operation is not performed, the system checks the media when a read/write operation is initiated in the drive.

Cleaning Stand-Alone Drives

The following section applies only to stand-alone drives and is not applicable for removable disk drives.

You must manually clean the stand-alone drives, whenever necessary. The **Clean Drive** option is not provided for stand-alone drives. However, after manually cleaning the stand-alone drives, you must mark the drive as cleaned using the **Mark Drive Cleaned** option. This will reset the counters that keep track of the number of events that have occurred since the drive was cleaned. For more information on marking a drive as cleaned, see Mark Drive Cleaned.

GridStor and Stand-Alone Drives

Stand-alone drives can be used to configure Alternate Data Paths (GridStor). Typical scenario in which this feature is useful is when a production site is backed up and restored to a DR site regularly using a stand-alone drive.

License Requirement

This feature requires a Feature License to be available in the CommServe® Server.

Review general license requirements included in License Administration. Also, View All Licenses provides step-by-step instructions on how to view the license information.

Back to Top

Stand-Alone Drives - Configure

Topics | Configure | How to | Troubleshoot | Related Topics

CONFIGURE A STAND-ALONE DRIVE

The following procedure describes the steps involved in configuring a stand-alone drive attached to a MediaAgent.

Required Capability: See Capabilities and Permitted Actions

BEFORE YOU BEGIN

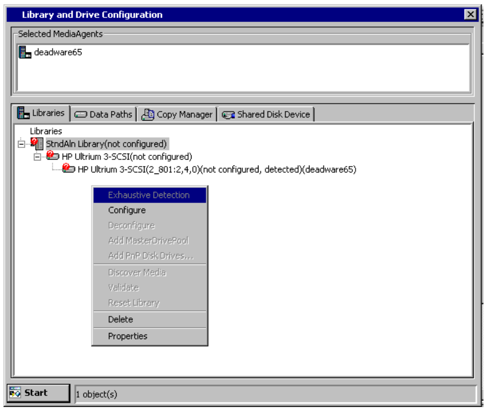
This feature requires a Feature License to be available in the CommServe® Server.

Review general license requirements included in License Administration. Also, View All Licenses provides step-by-step instructions on how to view the license information.

TO CONFIGURE A STAND-ALONE DRIVE

1. Display the Library and Drive Configuration window.
2. Detect the devices for the MediaAgent to which the stand-alone drive you wish to configure is attached. Detect the devices as described in Detect Devices.

   All the devices attached to the selected MediaAgent are displayed in the **Library and Drive Configuration** window.
3. Locate the library that you want to configure. If the library was never configured, the library and drive identifiers end in a # sign (i.e., Library#). If the library was configured and then deconfigured, the library and drive names are retained (e.g., Library2).



Library and Drive Configuration

Selected MediaAgents

deadware65

Libraries

StndAln Library(not configured)

HP Ultrium 3-SCSI(not configured)

HP Ultrium 3-SCSI(2_801:2,4,0)(not configured, detected)(deadware65)

1 object(s)

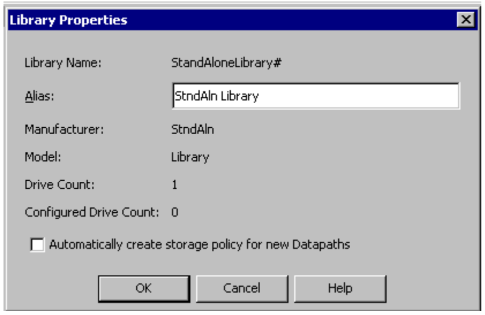
4. If you want to modify library properties, right-click the library and select Properties.

   You can change the following properties:

   Alias - The name of the library. This name is displayed in the CommCell Browser for the library.

   We strongly recommend that you provide appropriate labels or aliases for each stand-alone drive . This will help you identify the proper drive when you are prompted to insert media into a drive.

   When you are satisfied with your changes, click **OK**.



Library Properties

Library Name: StandAloneLibrary#

Alias: StndAln Library

Manufacturer: StndAln

Model: Library

Drive Count: 1

Configured Drive Count: 0

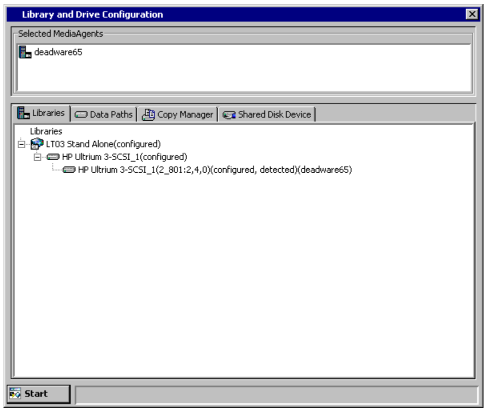
☐ Automatically create storage policy for new Datapaths

We recommend that you give each library a descriptive name as its Alias, for easier system administration. For stand-alone drives, we strongly recommend that you physically label each drive using the library name shown in the configuration window. This will help you identify the proper drive when you are prompted to insert a cartridge into a drive.

5. When you are satisfied with your changes, click **OK**.

6. In the **Library and Drive Configuration** window, right-click the library that you want to configure, and then click **Configure**.
7. A prompt appears, asking if you are sure that you want to configure the library. Click **Yes** to continue with the configuration.

   The status of the library changes to configured.



deadware65

Libraries
LT03 Stand Alone(configured)
HP Ultrium 3-SCSI_1(configured)
HP Ultrium 3-SCSI_1(2_801:2,4,0)(configured, detected)(deadware65)

Configure Multiple Stand-Alone Drives into a Drive Pool

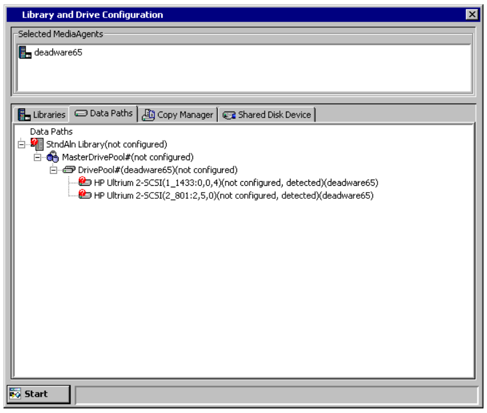
The following procedure describes the steps involved in configuring multiple stand-alone drives with the same drive type attached to a MediaAgent. For an overview of this operation, see Drive Pooling Stand-Alone Drives.

Required Capability: See Capabilities and Permitted Actions

TO CONFIGURE MULTIPLE STAND-ALONE DRIVES INTO A DRIVE POOL

1. Display the Library and Drive Configuration window.
2. Detect the devices for the MediaAgent to which the stand-alone drive you wish to configure is attached. Detect the devices as described in Detect Devices.

   All the devices attached to the selected MediaAgent are displayed in the **Library and Drive Configuration** window.



deadware65

Data Paths
StndAln Library(not configured)
MasterDrivePool#(not configured)
DrivePool#(deadware65)(not configured)
HP Ultrium 2-SCSI(1_1433:0,0,4)(not configured, detected)(deadware65)
HP Ultrium 2-SCSI(2_801:2,5,0)(not configured, detected)(deadware65)

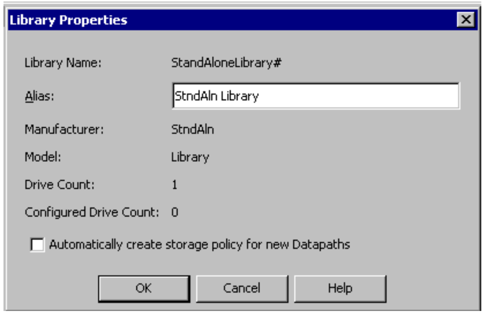
3. If you want to modify library properties, right-click the library and then click **Properties**.

   You can change the following properties:

   Alias - The name of the library. This name is displayed in the CommCell Browser for the library.

   We strongly recommend that you provide appropriate labels or aliases for each stand-alone drive . This will help you identify the proper drive when you are prompted to insert media into a drive.

   When you are satisfied with your changes, click **OK**.



Library Name: StandAloneLibrary#

Alias: StndAln Library

Manufacturer: StndAln

Model: Library

Drive Count: 1

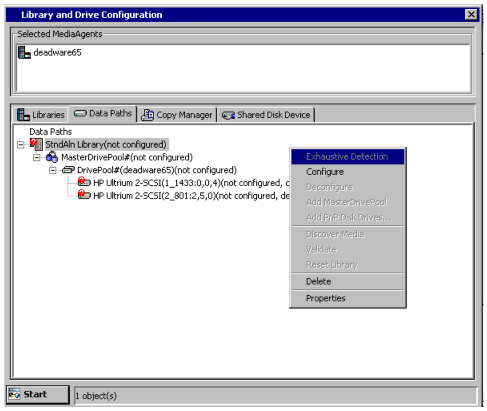
Configured Drive Count: 0

☐ Automatically create storage policy for new Datapaths

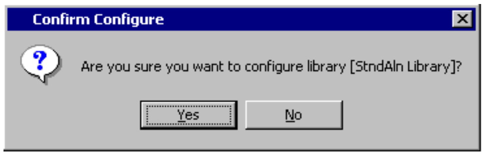
We recommend that you give each library a descriptive name as its Alias, for easier system administration. For stand-alone drives, we strongly recommend that you physically label each drive using the library name shown in the configuration window. This will help you identify the proper drive when you are prompted to insert a cartridge into a drive.

4. In the **Library and Drive Configuration** window, right-click the library that you want to configure, and then click **Configure**.

   Locate the library that you want to configure. If the library was never configured, the library and drive identifiers end in a # sign (i.e., Library#). If the library was configured and then deconfigured, the library and drive names are retained (e.g., Library2).

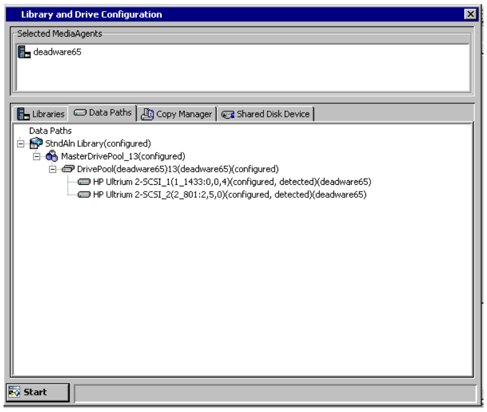


5. Click **Yes** to continue with the configuration.



Are you sure you want to configure library [StndAln Library]?

The status of the library changes to **configured**.


Library and Drive Configuration
Selected MediaAgents
deadware65
Libraries
Data Paths
Copy Manager
Shared Disk Device
Data Paths
StndAln Library(configured)
MasterDrivePool_13(configured)
DrivePool(deadware65)13(deadware65)(configured)
HP Ultrium 2-SCSI_1(1_1433:0,0,4)(configured, detected)(deadware65)
HP Ultrium 2-SCSI_2(2_801:2,5,0)(configured, detected)(deadware65)
Start

Drive Pooling Stand-Alone Drives That Were Previously Configured as Separate Stand-Alone Drives

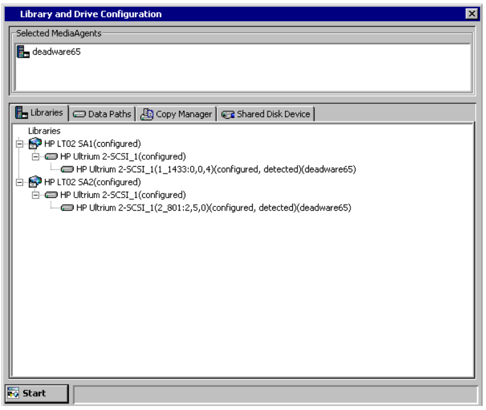
The following procedure describes the steps involved in re-configuring multiple stand-alone drives in a drive pool. Note that the stand-alone drives must be of the same drive type and attached to the same MediaAgent. For an overview of this operation, see Drive Pooling Stand-Alone Drives.

Required Capability: See Capabilities and Permitted Action

TO CONFIGURE MULTIPLE STAND-ALONE DRIVES INTO A DRIVE POOL

1. Display the Library and Drive Configuration window.

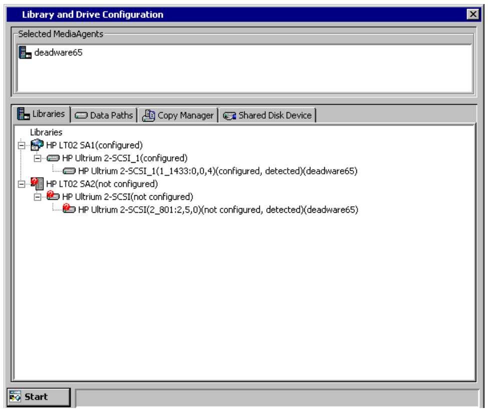
All the stand-alone drives that are currently configured will be displayed in the **Library and Drive Configuration** window.


Library and Drive Configuration
Selected MediaAgents
deadware65
Libraries
Data Paths
Copy Manager
Shared Disk Device
Libraries
HP LT02 SA1(configured)
HP Ultrium 2-SCSI_1(configured)
HP Ultrium 2-SCSI_1(1_1433:0,0,4)(configured, detected)(deadware65)
HP LT02 SA2(configured)
HP Ultrium 2-SCSI_1(configured)
HP Ultrium 2-SCSI_1(2_801:2,5,0)(configured, detected)(deadware65)
Start

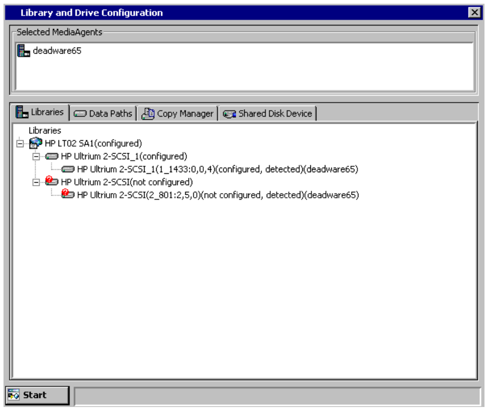
2. Deconfigure all the libraries, except one library associated with any of the stand-alone drives.

NOTES

- Click **Yes** in the **Confirm Deconfigure prompt** which appears when you deconfigure the library.
- If necessary, repeat this step to deconfigure all the libraries that will be used to create the drive pool - except one stand-alone library, as mentioned above.
- The deconfigured library will be displayed with the **not configured** status.


Library and Drive Configuration
Selected MediaAgents
deadware65
Libraries
Data Paths
Copy Manager
Shared Disk Device
Libraries
HP LT02 SA1(configured)
HP Ultrium 2-SCSI_1(configured)
HP Ultrium 2-SCSI_1(1_1433:0,0,4)(configured, detected)(deadware65)
HP LT02 SA2(not configured)
HP Ultrium 2-SCSI(not configured)
HP Ultrium 2-SCSI(2_801:2,5,0)(not configured, detected)(deadware65)
Start

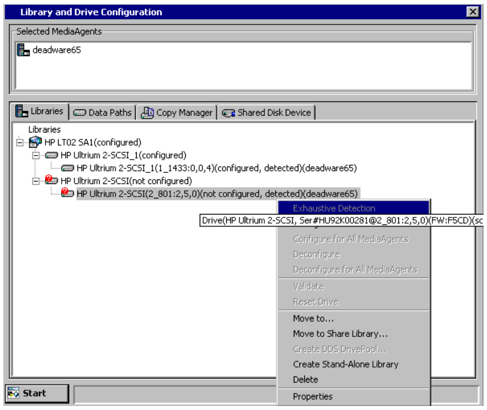
3. Delete the deconfigured drive. Detect the devices as described in Detect Devices.


Library and Drive Configuration
Selected MediaAgents
deadware65
Libraries
Data Paths
Copy Manager
Shared Disk Device
Libraries
HP LT02 SA1(configured)
HP Ultrium 2-SCSI_1(configured)
HP Ultrium 2-SCSI_1(1_1433:0,0,4)(configured, detected)(deadware65)
HP Ultrium 2-SCSI(not configured)
HP Ultrium 2-SCSI(2_801:2,5,0)(not configured, detected)(deadware65)
Start

4. Configure the drive that was detected.

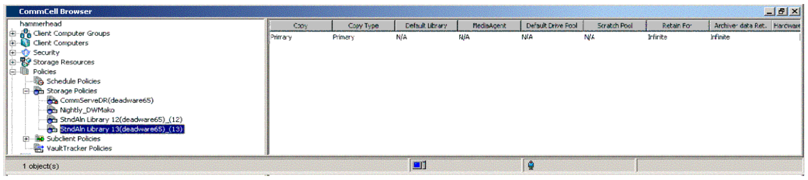
NOTES

- Click **Yes** in the **Confirm Configure** prompt which appears when you configure the drive.
- If necessary, repeat this step to configure all the drives that were detected.
- The drives are configured and displayed with the **configured** status.


Library and Drive Configuration
Selected MediaAgents
deadware65
Libraries
Data Paths
Copy Manager
Shared Disk Device
Libraries
HP LT02 SA1(configured)
HP Ultrium 2-SCSI_1(configured)
HP Ultrium 2-SCSI_1(1_1433:0,0,4)(configured, detected)(deadware65)
HP Ultrium 2-SCSI(not configured)
HP Ultrium 2-SCSI(2_801:2,5,0)(not configured, detected)(deadware65)
Exhaustive Detection
Drive(HP Ultrium 2-SCSI, Ser#HU92K00281@2_801:2,5,0)(FW:F5CD)(sc
Configure for All MediaAgents
Deconfigure
Deconfigure for All MediaAgents
Validate
Reset Drive
Move to...
Move to Share Library...
Create DDS DrivePool...
Create Stand-Alone Library
Delete
Properties
Start

POST CONFIGURATION CONSIDERATIONS

From the CommCell Browser, locate the Storage Policy associated with the deconfigured drives. In the right-pane of the CommCell Browser, right-click the primary copy and then click **Properties**.

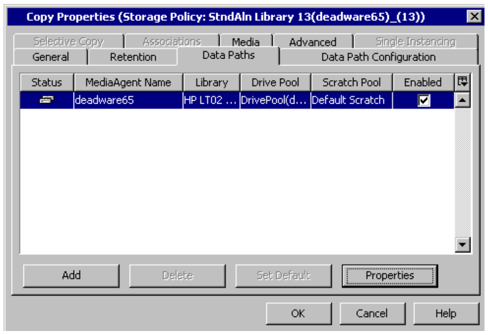


Copy	Copy Type	Default Library	MediaAgent	Default Drive Pool	Scratch Pool	Retain For	Archiver data Ret.	Hardware
Primary	Primary	N/A	N/A	N/A	N/A	Infinite	Infinite	

From the **Data Path** tab of the **Copy Properties** dialog box, add the data path associated with the library in which the drive is currently drive pooled as the alternate data path. (See Add a Data Path to a Storage Policy Copy for step-by-step instructions.)

NOTES

- If necessary, repeat this step to add the data path in all the storage policies associated with the drives that were deconfigured.



Copy Properties (Storage Policy: StndAln Library 13(deadware65)_(13))

Status	MediaAgent Name	Library	Drive Pool	Scratch Pool	Enabled
	deadware65	HP LT02 ...	DrivePool(d...	Default Scratch	☑

CONFIGURE A STAND-ALONE DRIVE SHARED ACROSS A SAN (DDS)

The following procedure describes the steps involved in configuring a Stand-Alone drive that is shared across a SAN with DDS.

BEFORE YOU BEGIN

Check the following before you configure the library in the SAN environment:

- Hardware is configured according to the conventions detailed in Hardware Configuration Guidelines - Libraries Attached to a SAN.
- MediaAgent software is installed on every computer that is connected to the SAN, and that will access the library. The MediaAgent software can be installed on the computers in any order; the installation sequence does not affect the library configuration.
- This feature requires a Feature License to be available in the CommServe® Server.

  Review general license requirements included in License Administration. Also, View All Licenses provides step-by-step instructions on how to view the license information.

TO CONFIGURE A STAND-ALONE DRIVE ACROSS A SAN (DDS)

1. Display the Library and Drive Configuration window.

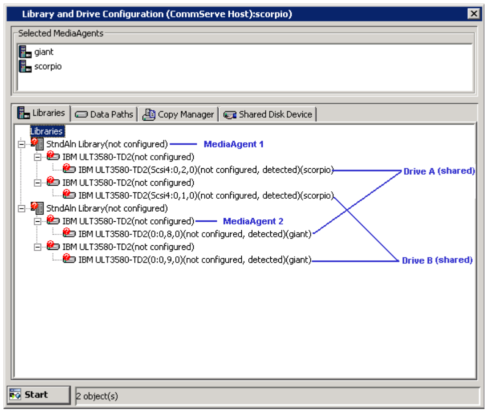
   In the **Select MediaAgents** dialog box, select the names of all the MediaAgents that will share the stand-alone drive.

2. Detect the devices. Use Detection or Exhaustive Detection as required.

   The stand-alone drives connected to the selected MediaAgents across the SAN will be displayed in the **Library and Drive Configuration** window.

   NOTE: If you have MediaAgent 1 and MediaAgent 2 sharing Drive A and Drive B, then the drives should appear twice, once associated with MediaAgent 1 and once associated with MediaAgent 2.

   The sample image represents a similar configuration.



Library and Drive Configuration (CommServe Host):scorpio)

Selected MediaAgents

giant
scorpio

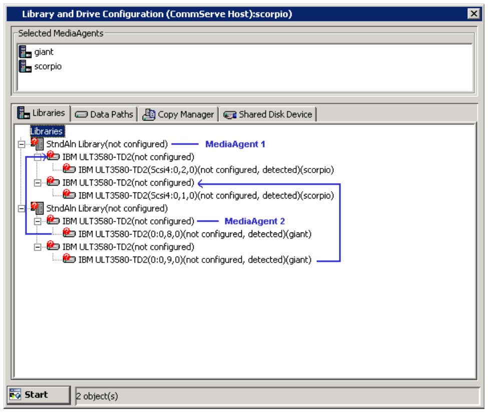
Libraries
StndAln Library(not configured)
IBM ULT3580-TD2(not configured)
IBM ULT3580-TD2(Scsi4:0,2,0)(not configured, detected)(scorpio)
IBM ULT3580-TD2(not configured)
IBM ULT3580-TD2(Scsi4:0,1,0)(not configured, detected)(scorpio)
StndAln Library(not configured)
IBM ULT3580-TD2(not configured)
IBM ULT3580-TD2(0:0,8,0)(not configured, detected)(giant)
IBM ULT3580-TD2(not configured)
IBM ULT3580-TD2(0:0,9,0)(not configured, detected)(giant)

2 object(s)

3. The drives from the stand-alone libraries must be grouped together.

   Drag the Drive A associated MediaAgent 2 and drop it together with the Drive A associated with MediaAgent 1 (into the other stand-alone library). Similarly, drag and drop Drive B.

   The sample image illustrates the drag and drop.



Library and Drive Configuration (CommServe Host):scorpio)

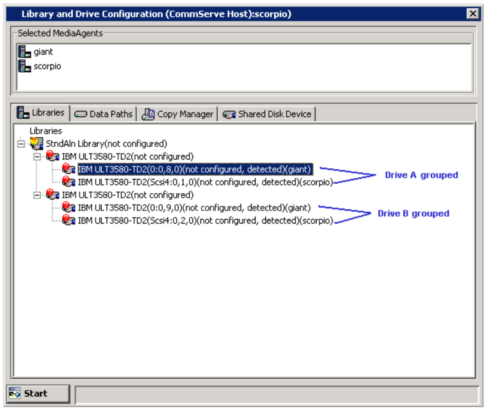
Selected MediaAgents

giant
scorpio

Libraries
StndAln Library(not configured)
IBM ULT3580-TD2(not configured)
IBM ULT3580-TD2(Scsi4:0,2,0)(not configured, detected)(scorpio)
IBM ULT3580-TD2(not configured)
IBM ULT3580-TD2(Scsi4:0,1,0)(not configured, detected)(scorpio)
StndAln Library(not configured)
IBM ULT3580-TD2(not configured)
IBM ULT3580-TD2(0:0,8,0)(not configured, detected)(giant)
IBM ULT3580-TD2(not configured)
IBM ULT3580-TD2(0:0,9,0)(not configured, detected)(giant)

2 object(s)

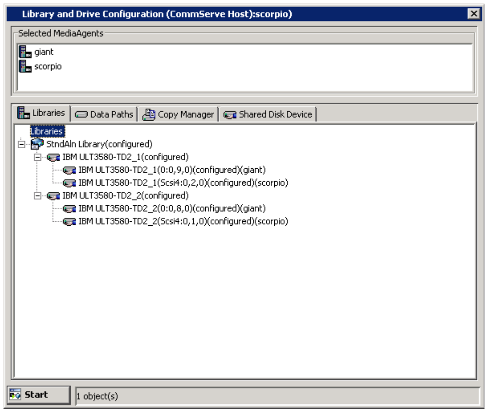
After moving the drives, the standalone library the drives under the standalone library should look similar to the sample image.


Library and Drive Configuration (CommServe Host):scorpio)
Selected MediaAgents
giant
scorpio
Libraries
Data Paths
Copy Manager
Shared Disk Device
Libraries
StndAln Library(not configured)
IBM ULT3580-TD2(not configured)
IBM ULT3580-TD2(0:0,8,0)(not configured, detected)(giant)
IBM ULT3580-TD2(Scsi4:0,1,0)(not configured, detected)(scorpio)
IBM ULT3580-TD2(not configured)
IBM ULT3580-TD2(0:0,9,0)(not configured, detected)(giant)
IBM ULT3580-TD2(Scsi4:0,2,0)(not configured, detected)(scorpio)
Drive A grouped
Drive B grouped
Start

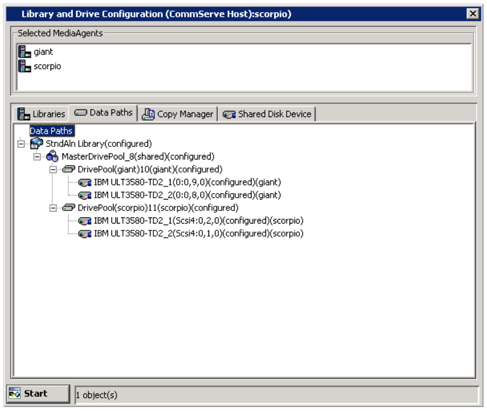
4. Configure the library as described in Configure Devices.

The library is configured and displayed with the **configured, detect success** status in the **Library and Drive Configuration** window.

The **Library** tab provides the physical view of the devices (library and drives).


Library and Drive Configuration (CommServe Host):scorpio)
Selected MediaAgents
giant
scorpio
Libraries
Data Paths
Copy Manager
Shared Disk Device
Libraries
StndAln Library(configured)
IBM ULT3580-TD2_1(configured)
IBM ULT3580-TD2_1(0:0,9,0)(configured)(giant)
IBM ULT3580-TD2_1(Scsi4:0,2,0)(configured)(scorpio)
IBM ULT3580-TD2_2(configured)
IBM ULT3580-TD2_2(0:0,8,0)(configured)(giant)
IBM ULT3580-TD2_2(Scsi4:0,1,0)(configured)(scorpio)
Start
1 object(s)

The **Data Paths** tab provides a logical view of the data path used to access the devices - library, master drive pool, drive pool, drive.


Library and Drive Configuration (CommServe Host):scorpio)
Selected MediaAgents
giant
scorpio
Libraries
Data Paths
Copy Manager
Shared Disk Device
Data Paths
StndAln Library(configured)
MasterDrivePool_8(shared)(configured)
DrivePool(giant)10(giant)(configured)
IBM ULT3580-TD2_1(0:0,9,0)(configured)(giant)
IBM ULT3580-TD2_2(0:0,8,0)(configured)(giant)
DrivePool(scorpio)11(scorpio)(configured)
IBM ULT3580-TD2_1(Scsi4:0,2,0)(configured)(scorpio)
IBM ULT3580-TD2_2(Scsi4:0,1,0)(configured)(scorpio)
Start
1 object(s)

Stand-Alone Drives - How To

Topics | Configure | How To | Troubleshoot | Related Topics

Media Labeling in Stand-Alone Drives

- Create Automatic Labeling Schemes
- Manually Add Media Identifiers (Stamp Media)

Detecting Media Changes in Stand-Alone Drives

- Setup Automatic Checking of Media
- Verify Media
- Enable (or Disable) Automatic Use of Spare Media from Different Scratch Pools
- Enable (or Disable) Unloading of Media from a Stand-alone Drive when Different Media is Required

Other Options

- Enable (or Disable) Media Related Pop-Ups in the CommCell Console
- Modify the Unmount Time for Inactive Media in the Drive
- Modify the Barcode and Location for a Media Associated with a Stand-Alone Drive

CREATE AUTOMATIC LABELING SCHEMES

Related Topic

- Automatic Labeling Schemes

Required Capability: See Capabilities and Permitted Actions

➡ To create automatic labeling schemes for stand-alone drives:

1. From the CommCell Browser, right-click the library for which you wish to create the labeling schemes and then click **Properties**.
2. Click the Media tab.
3. From the **Barcode Labeling Scheme** region, select the label and then click **Add Token**. The selected label is displayed in the box at the bottom of the region.
4. Click **OK** to save the changes.

ADD MEDIA IDENTIFIERS (STAMP MEDIA)

Required Capability: See Capabilities and Permitted Actions

➡ To add media identifiers for media associated with stand-alone drives:

1. From the CommCell Browser, right-click the library (stand-alone drive or PnP drive) for which you wish to add the identifiers, and then click **Stamp Media**.
2. In the Stamp Media dialog box specify whether the labeling scheme should be used or enter the barcode number or a unique identifier for the media.
3. Click **OK**.

   The media is listed in the **Default Scratch** pool.

SETUP AUTOMATIC CHECKING OF MEDIA

Related Topic

- Setting-Up Automatic Labeling Schemes

Required Capability: See Capabilities and Permitted Actions

➡ To setup automatic checking of media in stand-alone drives:

1. From the CommCell Browser, right-click the library for which you wish to modify this parameter and then click **Properties**.
2. Click the Drive tab.
3. Click on **Check for media change in drive every n minute(s)** option and specify the minutes.
4. Click **OK** to save the changes.

VERIFY MEDIA

Related Topic

- Detecting Media Changes in Stand-Alone Drives

Required Capability: See Capabilities and Permitted Actions

➡ To verify media in stand-alone drives:

1. From the CommCell Browser, right-click the media in the stand-alone drive and then click **Verify Media**.
2. The system verifies the media and then displays the media information in the **Verify Media** dialog box. Click **OK** to close the dialog box.

ENABLE (OR DISABLE) AUTOMATIC USE OF SPARE MEDIA FROM DIFFERENT SCRATCH POOLS

Required Capability: See Capabilities and Permitted Actions

▶ To enable (or disable) automatic use of spare media from different scratch pools:

1. From the CommCell Browser, right-click the library for which you wish to enable or disable this option then click **Properties**.
2. Click the Media tab.
3. Select the **Automatically use spare media from different scratch pool if found in drive** to enable the option, or clear the option to disable it.
4. Click **OK** to save the changes.

ENABLE (OR DISABLE) UNLOADING OF MEDIA FROM A STAND-ALONE DRIVE WHEN DIFFERENT MEDIA IS REQUIRED

Required Capability: See Capabilities and Permitted Actions

▶ To enable (or disable) unloading of media from a stand-alone drive when different media is required:

1. From the CommCell Browser, right-click the library for which you wish to enable or disable this option then click **Properties**.
2. Click the Media tab.
3. Select the **Unload media in standalone drive when different media is required** to enable the option, or clear the option to disable it.
4. Click **OK** to save the changes.

ENABLE (OR DISABLE) MEDIA RELATED POP-UPS IN THE COMMCELL CONSOLE

Related Topics:

- Pop-up Messages in Stand-Alone Drives

Required Capability: See Capabilities and Permitted Actions

▶ To enable (or disable) media related pop-ups in the CommCell Console:

1. From the CommCell Browser, right-click the library for which you wish to enable or disable the pop-ups then click **Properties**.
2. Click the Media tab.
3. Click on **Show Media related pop-up messages on CommCell Console** to enable the option, or clear the option to disable it.
4. Click **OK** to save the changes.

MODIFY THE UNMOUNT TIME FOR INACTIVE MEDIA IN THE DRIVE

Required Capability: See Capabilities and Permitted Actions

▶ To modify the unmount time for inactive media in the drive:

1. From the CommCell Browser, right-click the library for which you wish to modify the unmount time for inactive media in the drive, and then click **Properties**.
2. Click the Media Usage tab.
3. From the **Unmount Media from the drive after (n) Minutes/Hours of inactivity** box, type the unmount time that you wish to establish and then choose minutes or hours.
4. Click **OK** to save the changes.

MODIFY THE BARCODE AND LOCATION FOR A MEDIA ASSOCIATED WITH A STAND-ALONE DRIVE

Required Capability: See Capabilities and Permitted Actions

▶ To modify the barcode and location for a media associated with a stand-alone drive

1. From the CommCell Browser, click on **Exported Media** or **Assigned Media** group associated with a stand-alone drive in which the media is available. All the media existing in the stand-alone drive are displayed on the right-pane of the CommCell browser
2. Right-click the media for which you want to modify the properties, and then click **Properties**.
3. In the **Barcode/ Identifier** box, type a new barcode/identifier for the media.

4. In the **Location** box, type the location in which the media is stored.
5. Click OK to save the changes.

Virtual Tape Libraries

Topics | Configure | Related Topics

A Virtual Tape Library (VTL) is a disk-based library that emulates the traditional tape devices and formats, and can be installed onto any disk space. Refer to the manufacturer's documentation to see if a disk-based storage subsystem supports VTL emulation mode. Follow the manufacturer's instructions to create the virtual tape library and make sure that the MediaAgent can detect the virtual arm changer and the drives created.

Contact your software provider for the latest list of virtual tape libraries supported.

The NearStore virtual tape libraries require special configuration. See the following sections for more information.

- Configure a NearStore Virtual Tape Library
- Export data from a NearStore VTL
- Restore data from a NearStore VTL

Virtual Tape Libraries - Configure

Topics | Configure | Related Topics

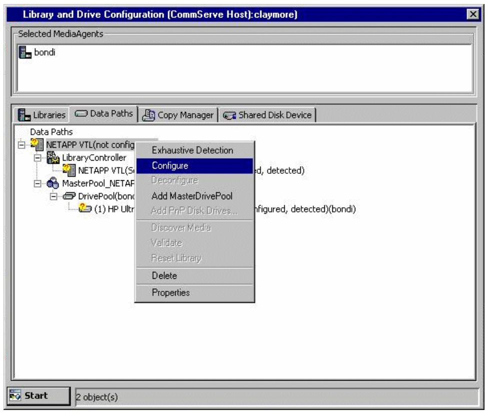
Configure a Virtual Tape library

Configure a NearStore Virtual Tape Library

- Export data from a NearStore VTL
- Restore data from a NearStore VTL

Configure a Virtual Tape Library

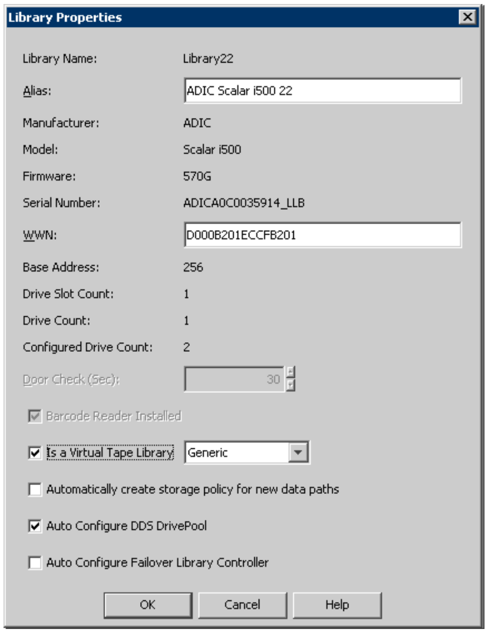
1. Follow the manufacturer's instructions to create the virtual tape library and make sure that the MediaAgent can detect the virtual arm changer and the drives created.
2. The virtual tape library can be configured using one of the following configurations:
   - Direct-attached library (See Direct-Attached Libraries - Configure for more information)
   - Direct-attached Shared (See Direct-Attached Shared Libraries - Configure for more information)
   - SAN-attached library (See SAN-Attached Libraries - Configure for more information)
3. Once configured right-click the library and then click **Properties**.



4. From the **Library Properties** window, select the **Is a Virtual Library Tape** option. Selecting this option ignores all the media and drive usage/cleaning thresholds that are not applicable to virtual tape libraries. Select **Generic** from the list.

   Click **OK**.

   Once configured, the virtual tape library supports most of the operations supported by actual tape library, depending on the manufacturer's implementation



Library Properties

Library Name: Library22

Alias: ADIC Scalar i500 22

Manufacturer: ADIC

Model: Scalar i500

Firmware: 570G

Serial Number: ADICA0C0035914_LLB

WWN: D000B201ECCFB201

Base Address: 256

Drive Slot Count: 1

Drive Count: 1

Configured Drive Count: 2

Door Check (Sec): 30

☑ Barcode Reader Installed

☑ Is a Virtual Tape Library: Generic

☐ Automatically create storage policy for new data paths

☑ Auto Configure DDS DrivePool

☐ Auto Configure Failover Library Controller

Configure a NearStore Virtual Tape Library

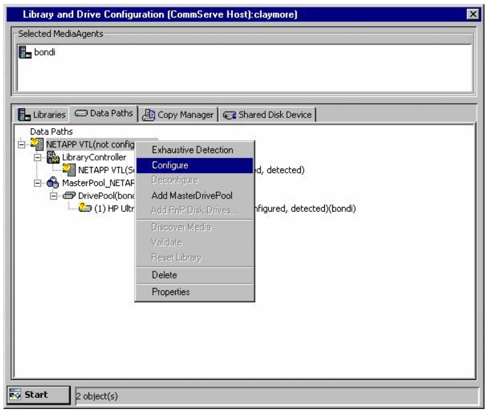
The NearStore virtual tape libraries require special configuration. See the following sections for details.

1. Follow the manufacturer's instructions to create the virtual tape library and make sure that the MediaAgent can detect the virtual arm changer and the drives created.

   Also make sure that you enable the shadow tape feature while creating the virtual tape, using the manufacturer's instructions.

2. The virtual tape library can be configured using one of the following configurations:
   - Direct-attached library (See Direct-Attached Libraries - Configure for more information)
   - Direct-attached Shared (See Direct-Attached Shared Libraries - Configure for more information)
   - SAN-attached library (See SAN-Attached Libraries - Configure for more information)

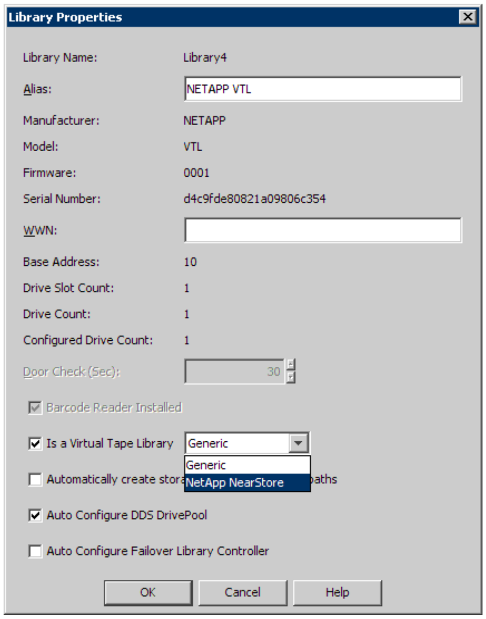
3. Once configured, to enable the shadow tape feature, right-click the library and then click **Properties**.



4. From the **Library Properties** window, select the **Is a Virtual Library Tape** option. Selecting this option ignores all the media and drive usage/cleaning thresholds that are not applicable to virtual tape libraries. Select **NetApp NearStore** from the list. Also select the **Barcode Reader Installed** option.

   Click **OK**. The shadow tape feature is now enabled in the virtual tape library.

   Once configured, the virtual tape library supports most of the operations supported by actual tape library, depending on the manufacturer's implementation



Library Properties

Library Name: Library4

Alias: NETAPP VTL

Manufacturer: NETAPP

Model: VTL

Firmware: 0001

Serial Number: d4c9fde80821a09806c354

WWN:

Base Address: 10

Drive Slot Count: 1

Drive Count: 1

Configured Drive Count: 1

Door Check (Sec): 30

☑ Barcode Reader Installed

☑ Is a Virtual Tape Library: Generic

□ Automatically create stor paths

☑ Auto Configure DDS DrivePool

□ Auto Configure Failover Library Controller

EXPORT DATA FROM A NEARSTORE VTL

When the virtual tape is exported to a physical tape, the physical media containing the matching barcode is loaded onto the physical library (if not already present), and the contents are copied from the virtual tape to physical tape. When this copy operation is complete, the virtual tape is marked as a shadow tape and this shadow tape is available for restore operations until the data expires.

RESTORE DATA FROM A NEARSTORE VTL

When the data from an exported virtual tape is restored, it would result in one of the following scenarios:

- Shadow tape is available

  In this scenario, the shadow tape is available in full, and the data is restored from the shadow tape.

- Shadow tape is not available, and the matching physical media is present in the library

  In this scenario, the shadow tape is recreated from the physical media containing the matching barcode, and the data is then restored from the recreated shadow tape.

- Shadow tape is not available, and the matching physical media is not present in the library

  In this scenario, the system will prompt the user to import the physical media containing the data. Once the media is imported into the physical library, the shadow tape is recreated from the physical media containing the matching barcode, and the data is then restored from the recreated shadow tape.

Once the restore operation is complete, it is highly recommended that you re-export the virtual tape back. This ensures that the virtual tape becomes shadow tape again, and the disk space reclaimed, if required.

It is recommended to schedule VaultTracker policies to periodically check and export full virtual tapes.

WORM Media

Topics | Configure | How To | Related Topics

Overview

WORM (Write-once-read-many) media are non rewritable data storage media. Once the WORM media is fully utilized, the media will not be recycled when it is pruned. It will be automatically moved to the **Retired Media** pool.

Tape libraries can be configured to use WORM media. If you plan to use WORM media, ensure that the **Automatically detect WORM Tape Media** option is enabled in the MediaAgents associated with the libraries in which you plan to use the WORM media.

License Requirement

This feature requires a Feature License to be available in the CommServe® Server.

Review general license requirements included in License Administration. Also, View All Licenses provides step-by-step instructions on how to view the license information.

Important Considerations

If you have any discovered spare WORM media in a Blind Library, then deconfiguring the library will leave the discovered spare WORM Media unusable. The media cannot be used when the library is configured back again. So apply caution when adding WORM media to a Blind Library for spare use.

WORM Media - Configure

Topics | Configure | How To | Related Topics

Configure a Library to Use WORM Media

Libraries with WORM Media can be configured using any of the tape library configurations described in the following sections:

- Direct-Attached Libraries
- Direct-Attached Shared Libraries
- SAN-Attached Libraries
- Stand-Alone Drives
- Optical Libraries
- Blind Libraries
- IP Libraries (Like libraries attached to ACSLS Server)

After configuring the library, perform the following steps to configure and manage WORM media in the library:

BEFORE YOU BEGIN

This feature requires a Feature License to be available in the CommServe® Server.

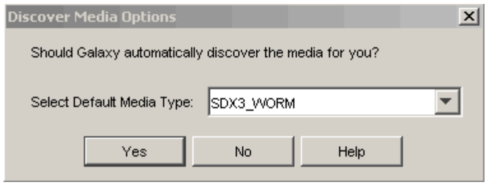
Review general license requirements included in License Administration. Also, View All Licenses provides step-by-step instructions on how to view the license information.

CONFIGURE A LIBRARY TO USE WORM MEDIA

1. Disable the option to automatically discover media from the library.

You can do this in one of the following ways:

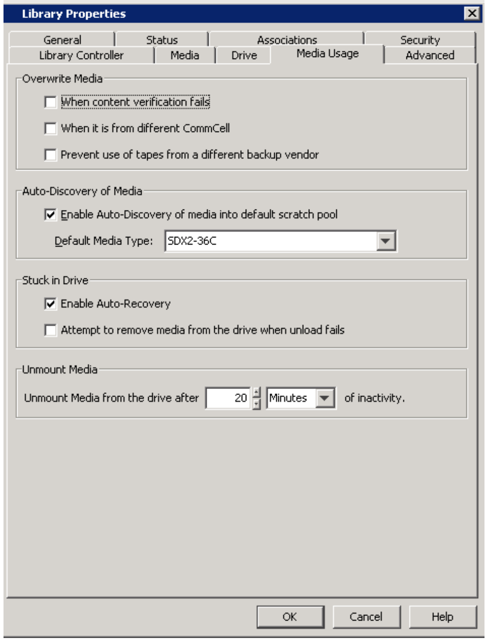
During the library configuration, you can disable the automatic media discovery, by clicking **No** in the **Discover Media Options** dialog box.


Discover Media Options

Should Galaxy automatically discover the media for you?

Select Default Media Type: SDX3_WORM

If the library is already configured to automatically discover media, disable the option from the **Media Usage** tab of the **Library Properties** dialog box.


Library Properties

Overwrite Media

☐ When content verification fails

☐ When it is from different CommCell

☐ Prevent use of tapes from a different backup vendor

Auto-Discovery of Media

☑ Enable Auto-Discovery of media into default scratch pool

Default Media Type: SDX2-36C

Stuck in Drive

☑ Enable Auto-Recovery

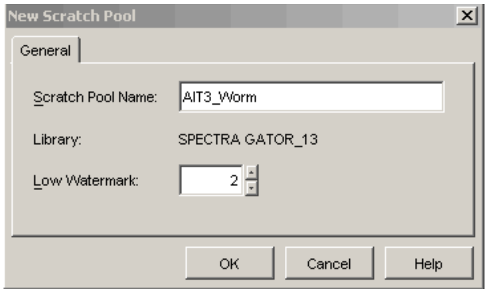
☐ Attempt to remove media from the drive when unload fails

Unmount Media

Unmount Media from the drive after 20 Minutes of inactivity.

2. From the **CommCell Console**, create new scratch pool(s) for the WORM media.

   See Creating New Scratch Pools for step-by-step information on how to create new scratch pools.


New Scratch Pool

Scratch Pool Name: AIT3_Worm

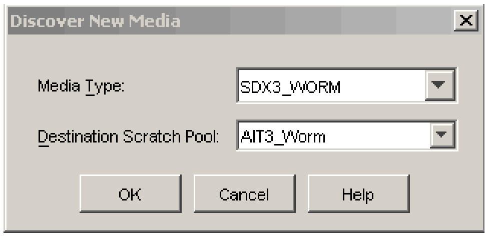
Library: SPECTRA GATOR_13

Low Watermark: 2

3. Manually discover the WORM media.

   See Discover a Specific Media Within a Library for step-by-step information on how to discover the media.

   Ensure that all the media is moved to the scratch pool created for WORM media.


Discover New Media

Media Type: SDX3_WORM

Destination Scratch Pool: AIT3_Worm

4. Create new Storage Policies, or re-associate existing Storage Policies to use the appropriate scratch pools.
5. Assign appropriate subclients to these Storage Policies.

WORM Media - How To

Topics | Configure | How To | Related Topics

ENABLE (OR DISABLE) AUTOMATIC DETECTION OF WORM MEDIA

Required Capability: Capabilities and Permitted Actions

➨ To enable or disable automatic detection of WORM media:

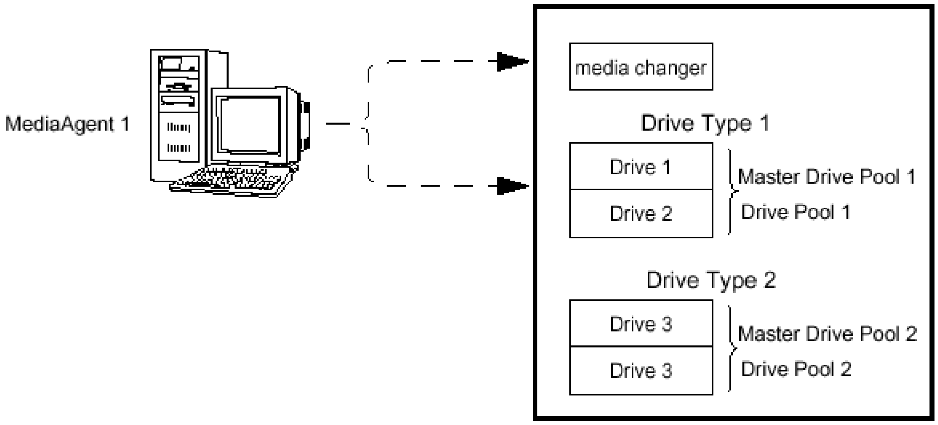
1. From the CommCell Browser, click the **MediaAgents** icon. All the MediaAgents available in the CommCell are displayed on the right-pane of the CommCell Browser.
2. Right-click the MediaAgent that you wish to enable (or disable) automatic detection of WORM media and then click **Properties**.
3. Click the Control tab.
4. Click and choose the **Automatically detect WORM Tape Media** option to enable automatic detection. (Clear the option to disable it.)
5. Click **OK** to save the configuration.

Libraries with Mixed Drive Types

Topics | Configure | Related Topics

Overview

Some libraries may have different or mixed drive types. Such drives may or may not use the same type of media. The following illustration represents a direct attached library configuration, with mixed drive type.



Note that the following functions are not supported by libraries with mixed drive types:

- Exhaustive Detection
- Verify Media

Also note that libraries with mixed drive types cannot be configured on Blind Libraries.

Libraries with Mixed Drive Types - Configure

Topics | Configure | Related Topics

Configure a Direct-Attached Library with Mixed Drive Types

Configure a Library with Mixed Drive Types in SAN

Configure a Direct-Attached Library with Mixed Drive Types

BEFORE YOU BEGIN

This feature requires a Feature License to be available in the CommServe® Server.

Review general license requirements included in License Administration. Also, View All Licenses provides step-by-step instructions on how to view the license information.

TO CONFIGURE A LIBRARY WITH MIXED DRIVE TYPES

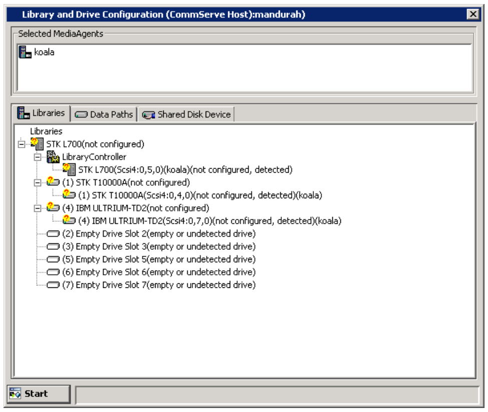
1. Display the Library and Drive Configuration window.
2. Detect the devices as described in Detect Devices.

   NOTES

   - Do not perform an exhaustive detection.

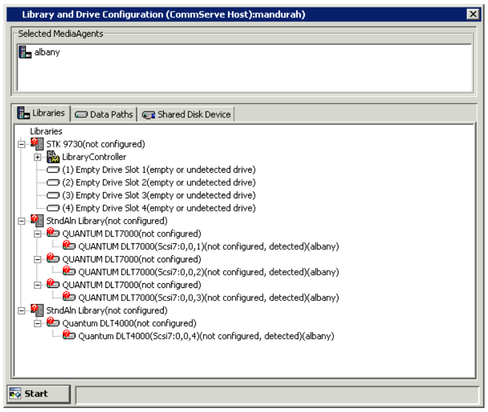
   If the library supports SCSI 3 drive identification, the system automatically detects the devices and displays them with detection status **detect success**, in the **Library and Drive Configuration** window.

   Note that the **Library and Drive Configuration** window displays a master drive pool (with a drive pool and the associated drives) for each of the drive types in the library.



```
koala

Libraries
STK L700(not configured)
    LibraryController
        STK L700(Scsi4:0,5,0)(koala)(not configured, detected)
    (1) STK T10000A(not configured)
        (1) STK T10000A(Scsi4:0,4,0)(not configured, detected)(koala)
    (4) IBM ULTRIUM-TD2(not configured)
        (4) IBM ULTRIUM-TD2(Scsi4:0,7,0)(not configured, detected)(koala)
    (2) Empty Drive Slot 2(empty or undetected drive)
    (3) Empty Drive Slot 3(empty or undetected drive)
    (5) Empty Drive Slot 5(empty or undetected drive)
    (6) Empty Drive Slot 6(empty or undetected drive)
    (7) Empty Drive Slot 7(empty or undetected drive)
```

If the library does not support SCSI 3 drive identification, the system detects the Library with **Empty Drive Slots** and the drives as **StndAln Library**.



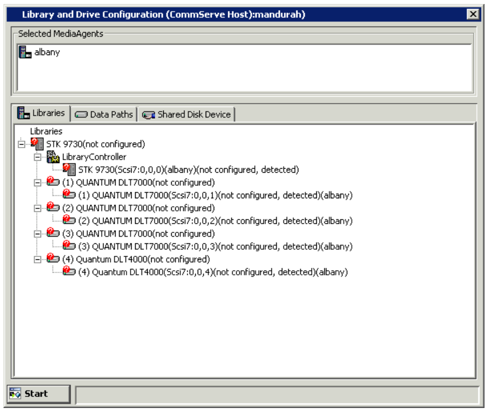
```
albany

Libraries
STK 9730(not configured)
    LibraryController
    (1) Empty Drive Slot 1(empty or undetected drive)
    (2) Empty Drive Slot 2(empty or undetected drive)
    (3) Empty Drive Slot 3(empty or undetected drive)
    (4) Empty Drive Slot 4(empty or undetected drive)
StndAln Library(not configured)
    QUANTUM DLT7000(not configured)
        QUANTUM DLT7000(Scsi7:0,0,1)(not configured, detected)(albany)
    QUANTUM DLT7000(not configured)
        QUANTUM DLT7000(Scsi7:0,0,2)(not configured, detected)(albany)
    QUANTUM DLT7000(not configured)
        QUANTUM DLT7000(Scsi7:0,0,3)(not configured, detected)(albany)
StndAln Library(not configured)
    Quantum DLT4000(not configured)
        Quantum DLT4000(Scsi7:0,0,4)(not configured, detected)(albany)
```

Map the drives to the appropriate drive slots, by dragging the standalone drives and dropping them on the appropriate drives.

NOTES

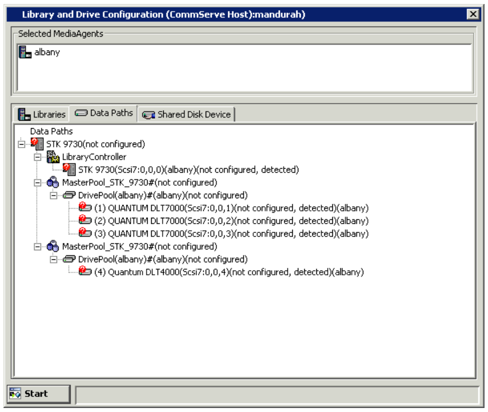
Physically verify the drives and the appropriate drive slot numbers before performing this operation in the **Library and Drive Configuration** window.

The **Library** tab provides the physical view of the devices (library and drives).



```
albany

Libraries
STK 9730(not configured)
    LibraryController
        STK 9730(Scsi7:0,0,0)(albany)(not configured, detected)
    (1) QUANTUM DLT7000(not configured)
        (1) QUANTUM DLT7000(Scsi7:0,0,1)(not configured, detected)(albany)
    (2) QUANTUM DLT7000(not configured)
        (2) QUANTUM DLT7000(Scsi7:0,0,2)(not configured, detected)(albany)
    (3) QUANTUM DLT7000(not configured)
        (3) QUANTUM DLT7000(Scsi7:0,0,3)(not configured, detected)(albany)
    (4) Quantum DLT4000(not configured)
        (4) Quantum DLT4000(Scsi7:0,0,4)(not configured, detected)(albany)
```

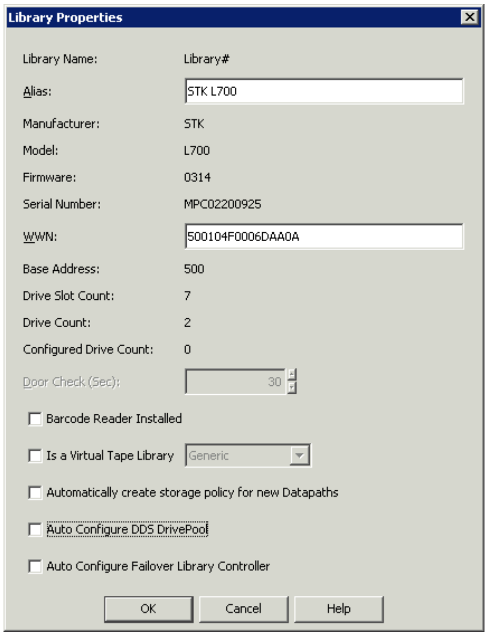
The **Data Paths** tab provides a logical view of the data path used to access the devices - library, master drive pool, drive pool, drive.



```
albany

Data Paths
STK 9730(not configured)
    LibraryController
        STK 9730(Scsi7:0,0,0)(albany)(not configured, detected)
    MasterPool_STK_9730#(not configured)
        DrivePool(albany)#(albany)(not configured)
            (1) QUANTUM DLT7000(Scsi7:0,0,1)(not configured, detected)(albany)
            (2) QUANTUM DLT7000(Scsi7:0,0,2)(not configured, detected)(albany)
            (3) QUANTUM DLT7000(Scsi7:0,0,3)(not configured, detected)(albany)
    MasterPool_STK_9730#(not configured)
        DrivePool(albany)#(albany)(not configured)
            (4) Quantum DLT4000(Scsi7:0,0,4)(not configured, detected)(albany)
```

3. Right-click the library and open the **Library Properties** window.

   Disable the option to **Automatically create storage policy for new DataPaths**.



Library Properties

Library Name: Library#

Alias: STK L700

Manufacturer: STK

Model: L700

Firmware: 0314

Serial Number: MPC02200925

WWN: 500104F0006DAA0A

Base Address: 500

Drive Slot Count: 7

Drive Count: 2

Configured Drive Count: 0

Door Check (Sec): 30

□ Barcode Reader Installed

□ Is a Virtual Tape Library Generic

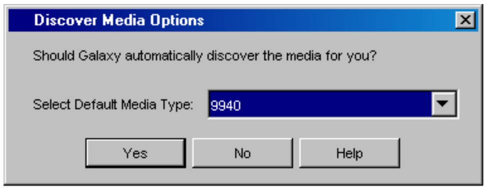
□ Automatically create storage policy for new Datapaths

□ Auto Configure DDS DrivePool

□ Auto Configure Failover Library Controller

4. Configure the library as described in Configure Devices.

If this **Discover Media Options** dialog box appears during the configuration process, click **No**.



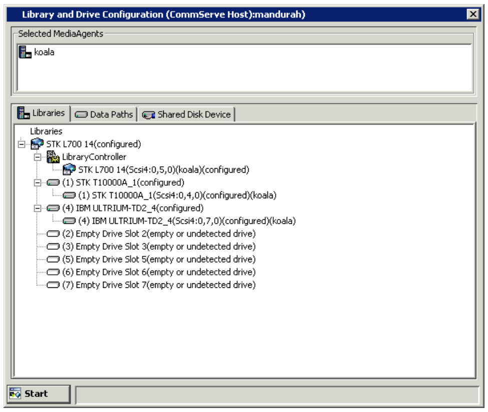
Discover Media Options

Should Galaxy automatically discover the media for you?

Select Default Media Type: 9940

The status of the library changes to **configured** in the **Library and Drive Configuration** window.

The **Library** tab provides the physical view of the devices (library and drives).

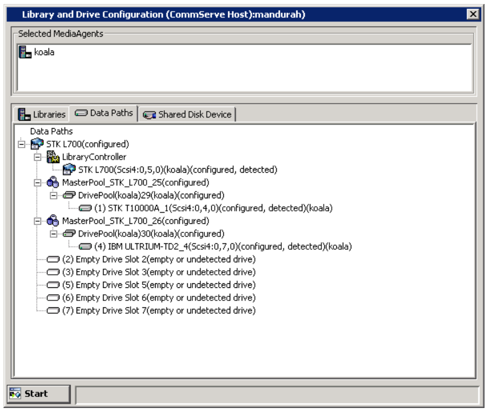


Library and Drive Configuration (CommServe Host):mandurah)

Selected MediaAgents: koala

```
Libraries
STK L700 14(configured)
    LibraryController
        STK L700 14(Scsi4:0,5,0)(koala)(configured)
    (1) STK T10000A_1(configured)
        (1) STK T10000A_1(Scsi4:0,4,0)(configured)(koala)
    (4) IBM ULTRIUM-TD2_4(configured)
        (4) IBM ULTRIUM-TD2_4(Scsi4:0,7,0)(configured)(koala)
    (2) Empty Drive Slot 2(empty or undetected drive)
    (3) Empty Drive Slot 3(empty or undetected drive)
    (5) Empty Drive Slot 5(empty or undetected drive)
    (6) Empty Drive Slot 6(empty or undetected drive)
    (7) Empty Drive Slot 7(empty or undetected drive)
```

The **Data Paths** tab provides a logical view of the data path used to access the devices - library, master drive pool, drive pool, drive.



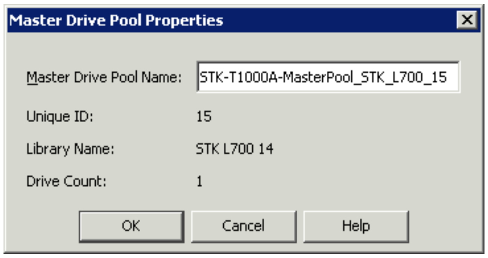
Library and Drive Configuration (CommServe Host):mandurah)

Selected MediaAgents: koala

```
Data Paths
STK L700(configured)
    LibraryController
        STK L700(Scsi4:0,5,0)(koala)(configured, detected)
    MasterPool_STK_L700_25(configured)
        DrivePool(koala)29(koala)(configured)
            (1) STK T10000A_1(Scsi4:0,4,0)(configured, detected)(koala)
    MasterPool_STK_L700_26(configured)
        DrivePool(koala)30(koala)(configured)
            (4) IBM ULTRIUM-TD2_4(Scsi4:0,7,0)(configured, detected)(koala)
    (2) Empty Drive Slot 2(empty or undetected drive)
    (3) Empty Drive Slot 3(empty or undetected drive)
    (5) Empty Drive Slot 5(empty or undetected drive)
    (6) Empty Drive Slot 6(empty or undetected drive)
    (7) Empty Drive Slot 7(empty or undetected drive)
```

5. Optionally, we recommend that you rename the Master Pools and Drive Pools with appropriate names, based on the drive type. This will help you to easily identify them later.

To rename a Master Pool, right-click the **MasterPool** from the **Data Path** tab and then click **Properties**. Type the new name and click **OK** to save.



Master Drive Pool Properties

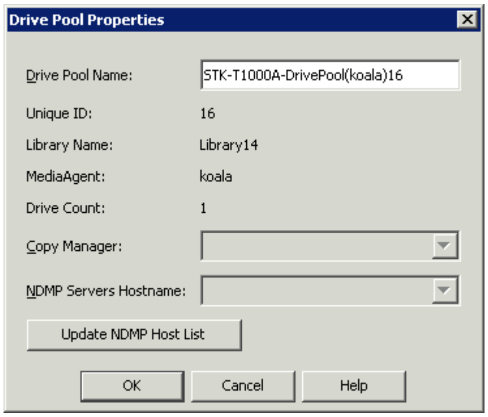
Master Drive Pool Name: STK-T1000A-MasterPool_STK_L700_15

Unique ID: 15

Library Name: STK L700 14

Drive Count: 1

To rename a Drive Pool, right-click the **DrivePool** from the **Data Path** tab and then click **Properties**. Type the new name and click **OK** to save.



Drive Pool Properties

Drive Pool Name: STK-T1000A-DrivePool(koala)16

Unique ID: 16

Library Name: Library14

MediaAgent: koala

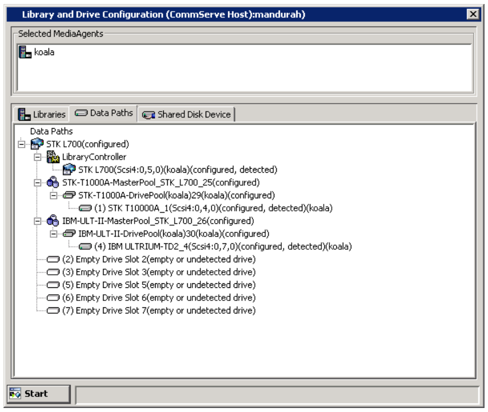
Drive Count: 1

Copy Manager:

NDMP Servers Hostname:

6. The changed names are reflected in the **Library and Drive Configuration** window.

   Exit the **Library and Drive Configuration** window. To exit, click the **Start** menu and then click **Exit**.



Library and Drive Configuration (CommServe Host):mandurah)

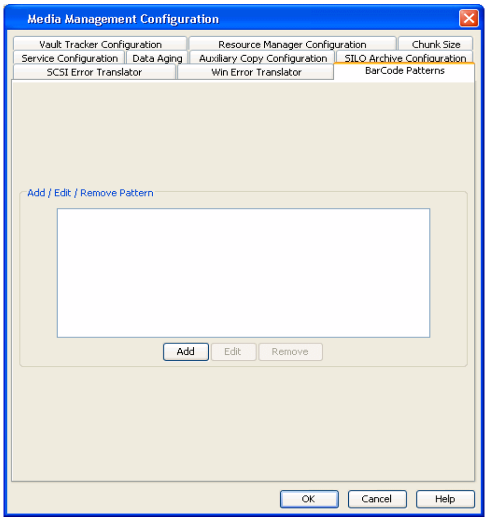
Selected MediaAgents

koala

```
Data Paths
STK L700(configured)
  LibraryController
    STK L700(Scsi4:0,5,0)(koala)(configured, detected)
  STK-T1000A-MasterPool_STK_L700_25(configured)
    STK-T1000A-DrivePool(koala)29(koala)(configured)
      (1) STK T10000A_1(Scsi4:0,4,0)(configured, detected)(koala)
  IBM-ULT-II-MasterPool_STK_L700_26(configured)
    IBM-ULT-II-DrivePool(koala)30(koala)(configured)
      (4) IBM ULTRIUM-TD2_4(Scsi4:0,7,0)(configured, detected)(koala)
  (2) Empty Drive Slot 2(empty or undetected drive)
  (3) Empty Drive Slot 3(empty or undetected drive)
  (5) Empty Drive Slot 5(empty or undetected drive)
  (6) Empty Drive Slot 6(empty or undetected drive)
  (7) Empty Drive Slot 7(empty or undetected drive)
```

7. From the CommCell Console, define the barcode patterns associated with the storage and cleaning media for each drive type.

   We highly recommend the usage of a specific barcode pattern for the media associated with each of the drive type in the library. This will help you to easily manage and administer the media in the library. (See Managing Barcodes in a Library for more information.)



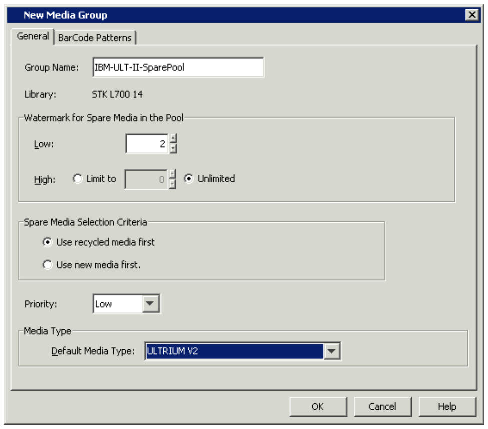
Media Management Configuration

Vault Tracker Configuration
Resource Manager Configuration
Chunk Size
Service Configuration
Data Aging
Auxiliary Copy Configuration
SILO Archive Configuration
SCSI Error Translator
Win Error Translator
BarCode Patterns
Add / Edit / Remove Pattern
Add
Edit
Remove
OK
Cancel
Help

8. Create new scratch media pools for the media associated with the various drive types.

   We recommend that you use appropriate names based on the drive type for each of the scratch media pools.

   Select the appropriate media type from the **Default Media Type** list.



New Media Group

General | BarCode Patterns

Group Name: IBM-ULT-II-SparePool

Library: STK L700 14

Watermark for Spare Media in the Pool

Low: 2

High: ○ Limit to 0 ● Unlimited

Spare Media Selection Criteria

● Use recycled media first

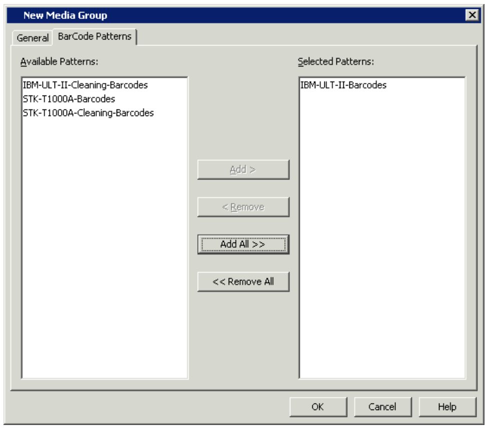
○ Use new media first.

Priority: Low

Media Type

Default Media Type: ULTRIUM V2

9. Associate the appropriate barcode pattern in each of these scratch media pools.



New Media Group

General | BarCode Patterns

Available Patterns:

IBM-ULT-II-Cleaning-Barcodes
STK-T1000A-Barcodes
STK-T1000A-Cleaning-Barcodes

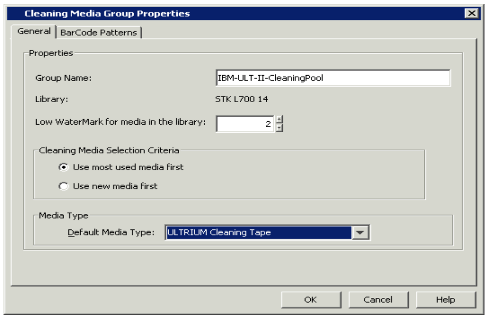
Selected Patterns:

IBM-ULT-II-Barcodes

10. Create new cleaning media pools for the cleaning media associated with the various drive types.

We recommend that you use appropriate names based on the drive type for each of the cleaning media pools.

Select the appropriate media type from the **Default Media Type** list.



Cleaning Media Group Properties

General | BarCode Patterns

Properties

Group Name: IBM-ULT-II-CleaningPool

Library: STK L700 14

Low WaterMark for media in the library: 2

Cleaning Media Selection Criteria

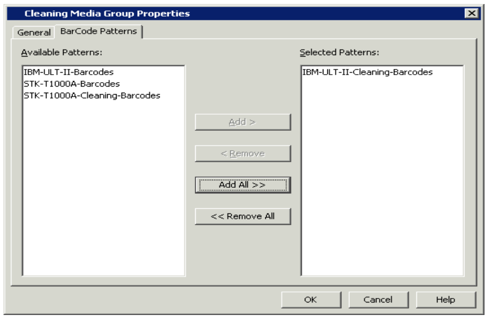
● Use most used media first

○ Use new media first

Media Type

Default Media Type: ULTRIUM Cleaning Tape

11. Associate the appropriate barcode pattern in each of these cleaning media pools.



Cleaning Media Group Properties

General | BarCode Patterns

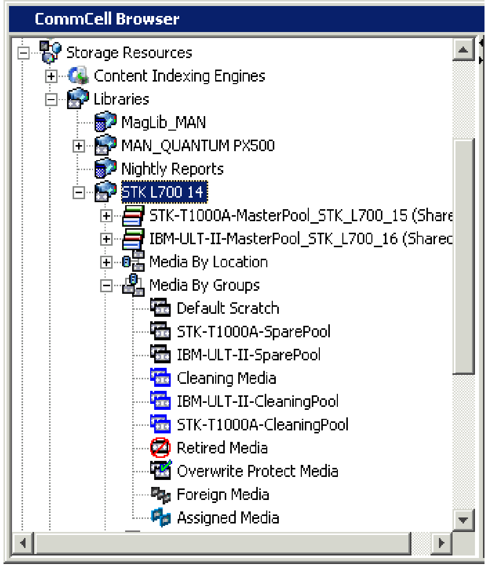
Available Patterns:

IBM-ULT-II-Barcodes
STK-T1000A-Barcodes
STK-T1000A-Cleaning-Barcodes

Selected Patterns:

IBM-ULT-II-Cleaning-Barcodes

The sample image shows the scratch and cleaning media pools with appropriate names associated with drives used in this example.



CommCell Browser

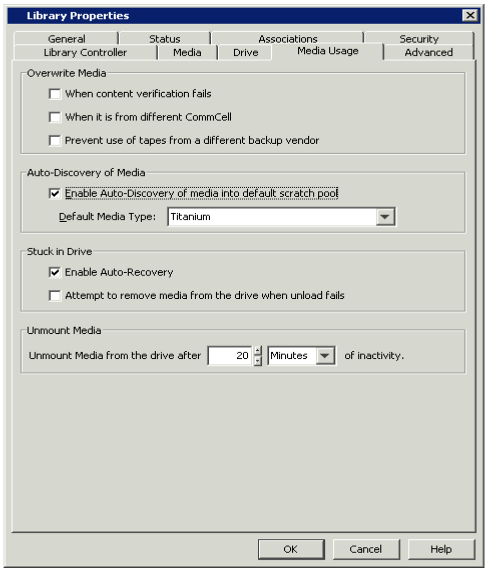
- Storage Resources
  - Content Indexing Engines
  - Libraries
    - MagLib_MAN
    - MAN_QUANTUM PX500
    - Nightly Reports
    - STK L700 14
      - STK-T1000A-MasterPool_STK_L700_15 (Share
      - IBM-ULT-II-MasterPool_STK_L700_16 (Sharec
      - Media By Location
      - Media By Groups
        - Default Scratch
        - STK-T1000A-SparePool
        - IBM-ULT-II-SparePool
        - Cleaning Media
        - IBM-ULT-II-CleaningPool
        - STK-T1000A-CleaningPool
        - Retired Media
        - Overwrite Protect Media
        - Foreign Media
        - Assigned Media

12. Open the Library Properties and enable the **Auto-Discovery of Media into default scratch pool** option.

    Select any one of the media as the **Default Media Type**.

    - If media is already available in the library, they will be automatically moved into the appropriate scratch pools. If the media is not moved, perform a Full Scan or Discover Media operation.
    - If media is not available in the library, the media will be automatically moved into appropriate scratch pools when you Import Media.

      If you import media that does not match the specified barcode patterns defined for the scratch pools, or is not of the media type associated with the defined scratch pools, the media will be moved to the default scratch pool. If necessary manually move them to the appropriate scratch pools.



Library Properties

Overwrite Media

□ When content verification fails

□ When it is from different CommCell

□ Prevent use of tapes from a different backup vendor

Auto-Discovery of Media

☑ Enable Auto-Discovery of media into default scratch pool

Default Media Type: Titanium

Stuck in Drive

☑ Enable Auto-Recovery

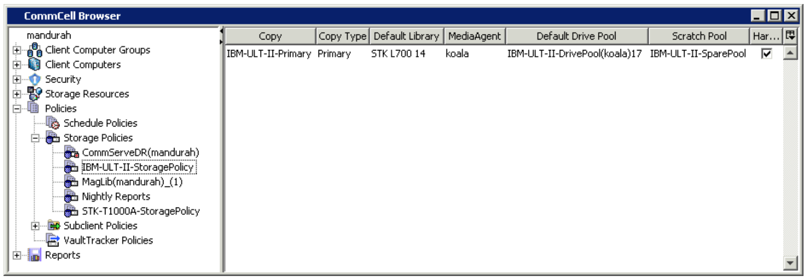
□ Attempt to remove media from the drive when unload fails

Unmount Media

Unmount Media from the drive after 20 Minutes of inactivity.

13. Create new Storage Policies using the appropriate naming convention as recommended earlier. Associate the Storage Policy Copies to use the appropriate drive pools and scratch pools.

    If you have existing storage policies, re-associate them to the appropriate drive pools and scratch pools.



CommCell Browser

- mandurah
  - Client Computer Groups
  - Client Computers
  - Security
  - Storage Resources
  - Policies
    - Schedule Policies
    - Storage Policies
      - CommServeDR(mandurah)
      - IBM-ULT-II-StoragePolicy
      - MagLib(mandurah)_(1)
      - Nightly Reports
      - STK-T1000A-StoragePolicy
    - Subclient Policies
    - VaultTracker Policies
  - Reports

Copy	Copy Type	Default Library	MediaAgent	Default Drive Pool	Scratch Pool	Har...
IBM-ULT-II-Primary	Primary	STK L700 14	koala	IBM-ULT-II-DrivePool(koala)17	IBM-ULT-II-SparePool	☑

POST CONFIGURATION CONSIDERATIONS

If you are configuring libraries with mixed drive types in a SAN do not enable the options to automatically configure the data paths in the Storage Policy Copy. (See To automatically configure the data paths in the Storage Policy Copy for more information.)

CONFIGURE A LIBRARY WITH MIXED DRIVE TYPES IN SAN

The following sections provide guidelines on configuring a library with mixed drive types in the SAN environment. (This procedure does not apply to NAS-attached libraries.)

CONSIDERATIONS FOR A LIBRARY WITH MIXED DRIVE TYPES IN SAN

1. Configure any of the MediaAgents sharing the library as described in Configure a Library with Mixed Drive Types.

2. After configuring the library: Display the Library and Drive Configuration window.

3. Open the **Library Properties** dialog box and select the following option:

   - **Auto Configure DDS DrivePool:** Enable this option to automatically configure the DDS drive pools for MediaAgents sharing these drives.

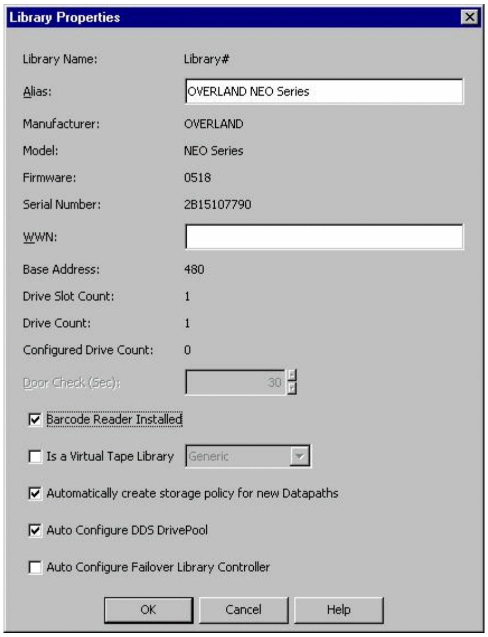
   Optionally, consider the following options:

   - **Auto Configure Failover Library Controllers**: Enable this option to automatically configure the Failover Library Controllers in all the MediaAgents sharing this library.
   - **Automatically create storage policy for new Datapaths**: Disable this option for libraries with mixed drive types.

   Click **OK**.

   NOTES

   - The option to automatically create/configure DDS DrivePools is not available for NAS-attached libraries; Dynamic Drive Sharing must be configured manually. For instructions on how to configure DDS for NAS-attached libraries, see Configure NAS-attached Libraries Shared Across a SAN .



Library Name: Library#

Alias: OVERLAND NEO Series

Manufacturer: OVERLAND

Model: NEO Series

Firmware: 0518

Serial Number: 2B15107790

WWN:

Base Address: 480

Drive Slot Count: 1

Drive Count: 1

Configured Drive Count: 0

Door Check (Sec): 30

☑ Barcode Reader Installed

☐ Is a Virtual Tape Library Generic

☑ Automatically create storage policy for new Datapaths

☑ Auto Configure DDS DrivePool

☐ Auto Configure Failover Library Controller

TO AUTOMATICALLY CONFIGURE THE OTHER MEDIAAGENTS THAT SHARE THE LIBRARY IN SAN

4. Install the library and ensure that the operating system detects the library. (See Driver Configurations for information on how to check this information for various operating systems.)

5. Install the MediaAgent software on all the other computers that will share the library. (See MediaAgent Deployment for information on installing the MediaAgent software.)

   If you have already installed the MediaAgent software, stop and start the MediaAgent Services on all the MediaAgents sharing this library.

   For more information on stopping and starting services, see the following topics:

   - Stop Services on Windows

     Start Services on Windows
   - Stop Services on Novell

     Start Services on Novell
   - Stop Services on Unix

     Start Services on Unix

   Open the Library and Drive Configuration window and verify that the libraries are configured from all the MediaAgents that share the library.

POST CONFIGURATION CONSIDERATIONS

Consider the following:

- When you create new storage policies, or have existing storage policies, ensure that the appropriate combination of drive pool and scratch pool are associated with them.
- Also when you configure the alternate data paths in a storage policy copy, ensure that the same combination of drive pool and scratch pool are added as the alternate paths .

Deconfiguring Libraries and Drives

Topics | How To | Related Topics

OVERVIEW

You may deconfigure a library or drive if:

- The device is irreparably damaged.
- You want to remove the library from the CommCell altogether.

Deconfiguring a library or drive disables software communications between the MediaAgent and the device. Deconfiguring a library also releases the license associated with the library.

You cannot carry out any operation (e.g., data protection, data recovery, maintenance operations) using a deconfigured library or drive. You can however re-use the media and the data available in the media by importing them to another library with similar or compatible drive types and then adding a data path to the new library from the storage policy copy that was originally used to perform data protection.

You can view the deconfigured libraries and the media (with contents) associated with the deconfigured libraries from the CommCell Console. See Delete Deconfigured Libraries.

> If you do not have library with compatible drive types in the CommCell, and wish to preserve the data for future restore/recover purposes, perform an Auxiliary Copy operation using another library to create secondary copies, before deconfiguring the library.

All the counters and history information associated with the library or drive will be lost, when it is deconfigured.

Consider the following, when you deconfigure libraries or drives:

- To re-use all the media in another library with similar or compatible drive types, add a data path to the new library from the storage policy copies that were originally used to perform data protection. (See View the Storage Policies Accessing a Library for step-by-step instructions on how to view the storage policies associated with a library.)

  You do not have to delete the storage policy to deconfigure the library. Keep in mind that all the data in the media will be lost and media will be recycled when a storage policy copy is deleted.

- Before you deconfigure a library, verify and ensure that none of the Storage Policy Copy's default data path points to the library. (See View the Storage Policies Accessing a Library for step-by-step instructions on how to view the storage policies associated with a library.) If necessary, set an alternate data path as the default data path before deconfiguring the library.

  If you have a storage policy copy with no default data path, use **Change Data Path** option to migrate the storage policy to point to another data path. See Change Data Path for more information.

- As the number of configured drives in a drive pool cannot be smaller than the largest number of streams used by any storage policy that accesses that drive pool, verify and if necessary reduce the number of streams in storage policy copies to be equal to the number of functional drives in the drive pool. For example, assume that a drive pool containing four drives is accessed by a four-stream storage policy. If you wish to deconfigure one of the drives, you must first reduce the four-streamed storage policies to three-streams.

  > Previous database backups using multiple streams cannot be restored if the number of streams in a storage policy is reduced.

- To re-use the storage policy associated with the deconfigured library, Change Data Path or Add a Data Path to a Storage Policy Copy.
- When you deconfigure the library from one of the MediaAgents that share a library in the SAN environment, check and verify that the **Auto Configure DDS DrivePool** and **Auto Configure Failover Library Controllers** options are disabled in the **Library Properties** dialog box in the **Library and Drive Configuration** window. If these options are not disabled, the system will automatically configure the library when the services in the MediaAgent are re-started.
- If you have any discovered spare WORM media in a Blind Library, then deconfiguring the library will leave the discovered spare WORM Media unusable. The media cannot be used when the library is configured back again. So apply caution when adding WORM media to a Blind Library for spare use.

Deconfiguring Libraries and Drives - How To

Topics | How To | Related Topics

DECONFIGURE LIBRARIES

Before you Begin

- Be certain that the library that you want to remove is not in use. Use the `Job Controller` to find and kill any jobs that use the library.
- Make sure that media is not mounted in the drives.

To deconfigure a library:

1. Display the Library and Drive Configuration window.
2. Right-click the library that you want to deconfigure, and then click **Deconfigure**.
3. A prompt appears, informing you that drives must be deconfigured before their library and asking if you want to deconfigure the library's drives. Click **Yes** to deconfigure.
4. A prompt appears, informing you that drive pools must be deconfigured before their library and asking if you want to deconfigure the library's drive pools. Click **Yes** to deconfigure.

The configuration status of the library, its drive pools, and its drives changes to **not configured**.

DELETE DECONFIGURED LIBRARIES

To delete a deconfigured library:

1. From the CommCell Console, right-click the deconfigured library that you want to delete, and then click **Delete**.
2. Click **Yes** in the Confirm prompt asking you whether you wish to delete the library.

The deconfigured library is deleted from the CommCell Console.

DECONFIGURE MASTER DRIVE POOLS

To deconfigure a master drive pool:

1. Display the Library and Drive Configuration window.
2. Deconfigure the drive pools associated with the master drive pool that you want to deconfigure. For more information see, Deconfiguring Drive Pools.
3. Right-click the master drive pool that you want to deconfigure, and then click **Deconfigure**.
4. A prompt appears, informing you that drives must be deconfigured before their drive pool and asking if you want to deconfigure the constituent drives. Click **Yes** to deconfigure.

   The configuration status of the master drive pool, its drive pools and their drives changes to **not configured**.

DECONFIGURE DRIVE POOLS

To deconfigure a drive pool:

1. Display the Library and Drive Configuration window.
2. Right-click the drive pool that you want to deconfigure, and then click **Deconfigure**.

3. A prompt appears, informing you that drives must be deconfigured before their drive pool and asking if you want to deconfigure the constituent drives. Click **Yes** to deconfigure.

   The configuration status of the drive pool and its drives changes to **not configured**.

DECONFIGURE DRIVES

Before you Begin

The number of configured drives in a drive pool cannot be smaller than the largest number of streams used by any storage policy that accesses that drive pool. For example, assume that a drive pool containing four drives is accessed only by a three-stream storage policy. In this case, you can deconfigure only one drive within the drive pool. The system prevents you from deconfiguring any additional drives. To deconfigure additional drives, you must first reduce the number of streams in the storage policy.

> Some Agents/database applications have the following requirement: The number of streams through which the database is restored must equal the number of streams through which the data was backed up. If you have used a storage policy for multi-stream database backups we advise you not to reduce the number of streams.

To deconfigure a drive:

1. Be certain that the drive that you want to deconfigure is not in use. Use the Job Controller to find and kill any jobs that use the drive. (For information on the killing a job from the Job Controller see Killing a Job.)
2. Make sure that a media is not mounted in the drive.
3. Display the Library and Drive Configuration window.
4. Right-click the drive that you want to deconfigure, and then click **Deconfigure**.
5. Click **Yes** in the confirmation prompt that appears to deconfigure the drive.

   The status of the drive changes to **not configured**.

Getting Started - Setup Deduplication

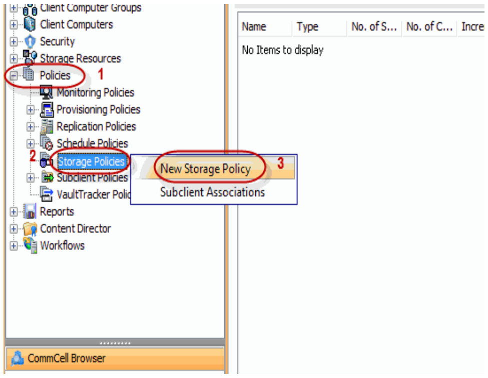
Disk Library | Shared Disk Library | Setup Deduplication

Previous Next

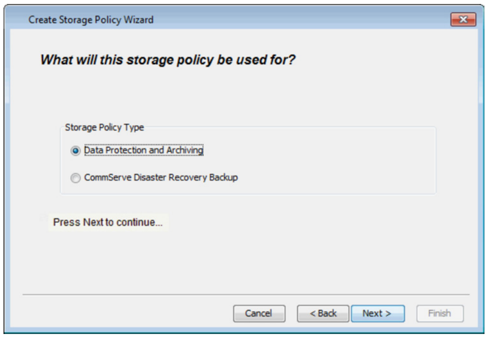
Make sure to read the Deduplication Building Block Guide before setting up deduplication.

Use the following steps to setup deduplication.

1.
- From the CommCell Browser, navigate to and expand **Policies**.
- Right-click **Storage Policies**, and then click **New Storage Policy**.



2. Click **Next**.



What will this storage policy be used for?

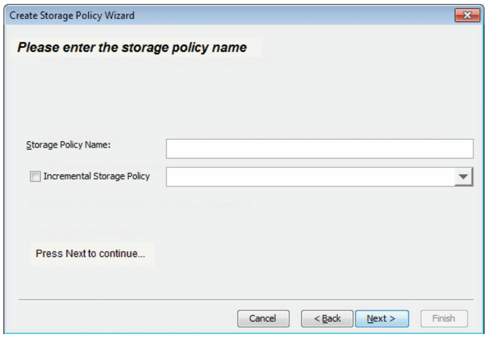
Storage Policy Type

● Data Protection and Archiving

○ CommServe Disaster Recovery Backup

Press Next to continue...

3. Enter the name in the **Storage Policy Name** box and click **Next**.



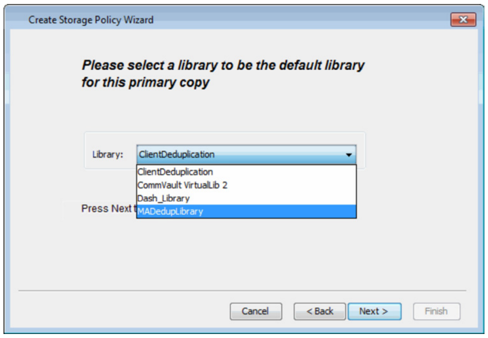
Please enter the storage policy name

Storage Policy Name:

□ Incremental Storage Policy

Press Next to continue...

4. From the **Library** list, click the name of a disk library and click **Next**.



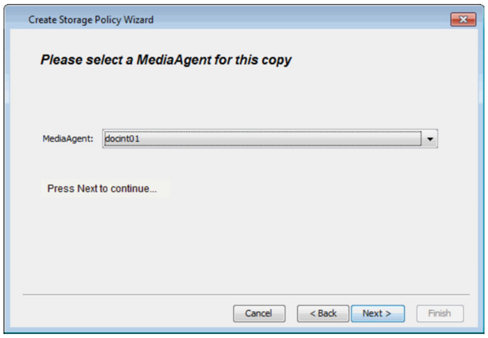
Please select a library to be the default library for this primary copy

Library: ClientDeduplication

Press Next

5. From the **MediaAgent** list, click the name of a MediaAgent that will be used to create the primary copy.

Click **Next**.



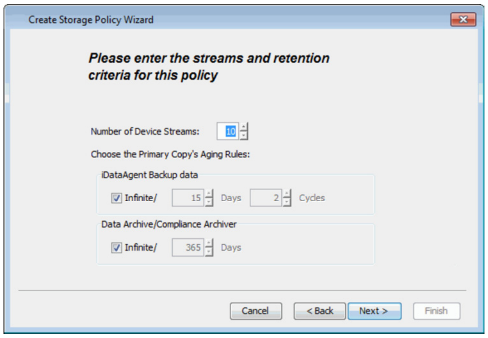
Please select a MediaAgent for this copy

MediaAgent: docint01

Press Next to continue...

6. Click **Next** to accept default values.

   If necessary these values can be modified later.



Please enter the streams and retention criteria for this policy

Number of Device Streams: 10

Choose the Primary Copy's Aging Rules:

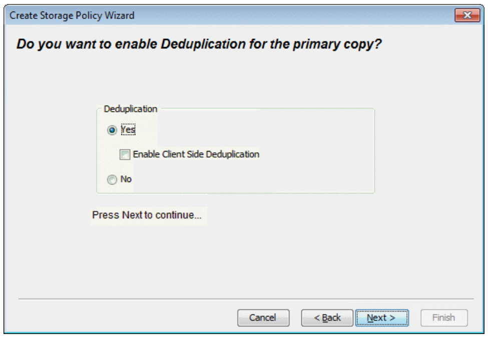
iDataAgent Backup data

☑ Infinite/ 15 Days 2 Cycles

Data Archive/Compliance Archiver

☑ Infinite/ 365 Days

7.
- Under **Deduplication**, select **Yes**.
- Clear **Enable Client Side Deduplication** check box and click **Next**.



Do you want to enable Deduplication for the primary copy?

Deduplication

● Yes

□ Enable Client Side Deduplication

○ No

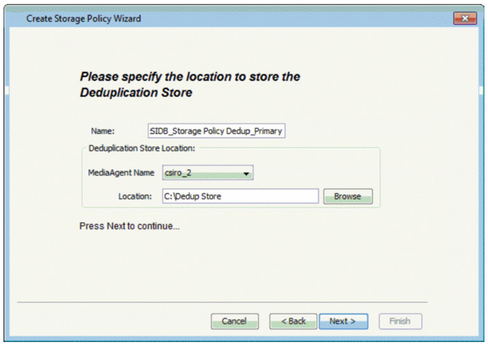
Press Next to continue...

8.
- From the **MediaAgent** list, click the name of the MediaAgent that will be used to store the Deduplication store.

  It can be any MediaAgent which has enough space to store the deduplication store.

- Type the name of the folder in which the deduplication database must be located in the **Deduplication Store Location** or click the **Browse** button to select the folder.
- Click **Next**.

  The deduplication database must be located in a folder and not directly under the root of a disk volume.



Please specify the location to store the Deduplication Store

Name: SIDB_Storage Policy Dedup_Primary

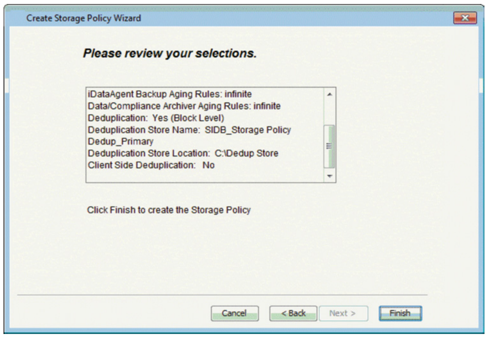
Deduplication Store Location:

MediaAgent Name csiro_2

Location: C:\Dedup Store

Press Next to continue...

9. Click **Finish**.

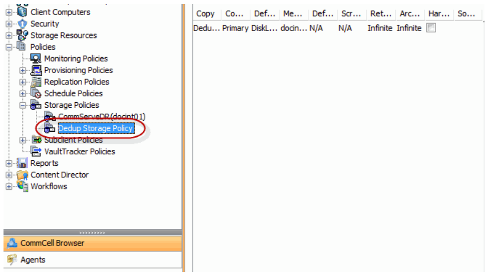


Please review your selections.

iDataAgent Backup Aging Rules: infinite
Data/Compliance Archiver Aging Rules: infinite
Deduplication: Yes (Block Level)
Deduplication Store Name: SIDB_Storage Policy Dedup_Primary
Deduplication Store Location: C:\Dedup Store
Client Side Deduplication: No

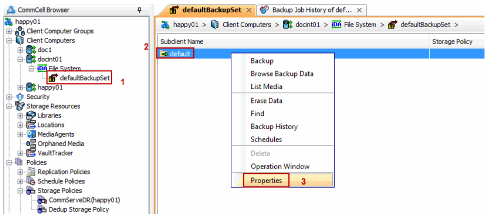
Click Finish to create the Storage Policy

10. You can view the storage policy under **Storage Policies** node.

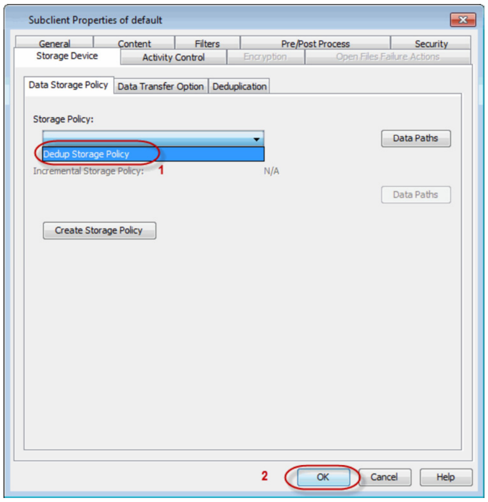


Copy	Co...	Def...	Me...	Def...	Scr...	Ret...	Arc...	Har...	So...
Dedu...	Primary	DiskL...	docin...	N/A	N/A	Infinite	Infinite	□	

11. - From the CommCell Browser, navigate to **Client Computers** | **<*Client*>** | **File System** | **defaultBackupSet**.
    - Right-click the subclient in the right pane and click **Properties**.



12. - Click the **Storage Device** tab.
    - In the **Storage Policy** list, click the storage policy where the MediaAgent Deduplication was enabled.
    - Click **OK**.

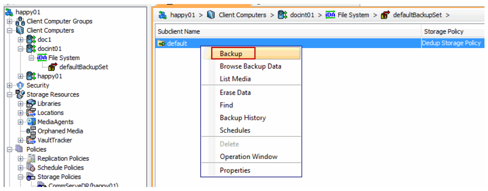


Storage Policy: Dedup Storage Policy

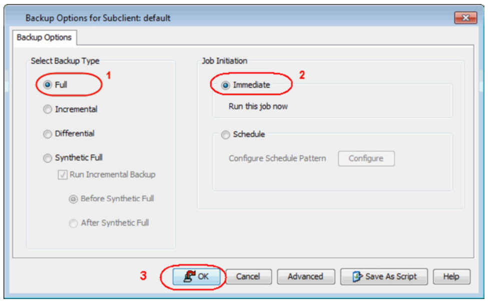
Incremental Storage Policy: N/A

13. - From the CommCell Browser, navigate to **Client Computer | <*Client*> | File System | defaultBackupSet**.
    - Right-click the subclient in the right pane and click **Backup**.

    The subclient should have at least 2GB of data to backup.

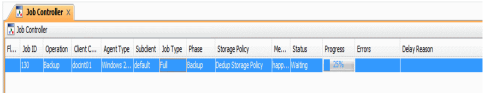


14. - Under **Select Backup Type**, click **Full**.
    - Under **Job Initiation**, click **Immediate**.
    - Click **OK**.



15. You can track the progress of the backup job from the **Job Controller** window.

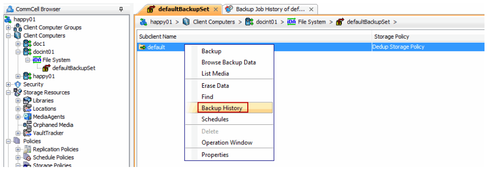
    Ensure that the job completes successfully.



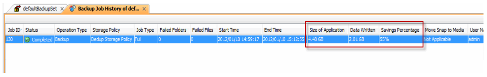
Fl...	Job ID	Operation	Client C...	Agent Type	Subclient	Job Type	Phase	Storage Policy	Me...	Status	Progress	Errors	Delay Reason
	130	Backup	docint01	Windows 2...	default	Full	Backup	Dedup Storage Policy	happ...	Waiting	26%		

16. - From the CommCell Browser, navigate to **Client Computers** | **<Client>** | **File System** | **defaultBackupSet**.
    - Right-click the subclient and click **Backup History**.
    - Click **OK**.
    - Note down the following deduplication details:

- Size of Application
- Data Written
- Savings Percentage



Subclient Name	Storage Policy
default	Dedup Storage Policy

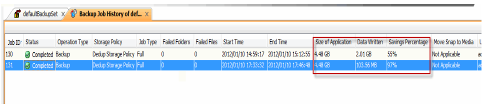


Job ID	Status	Operation Type	Storage Policy	Job Type	Failed Folders	Failed Files	Start Time	End Time	Size of Application	Data Written	Savings Percentage	Move Snap to Media	User N
130	Completed	Backup	Dedup Storage Policy	Full	0	0	2012/01/10 14:59:17	2012/01/10 15:12:55	4.48 GB	2.01 GB	55%	Not Applicable	admin

17. Repeat steps 13 - 15 and perform another Full backup to view the space savings due to deduplication.

18. Follow the steps in step 16 and the view the job history for the new job.

    You will notice the effect of deduplication as shown in the sample image.



Job ID	Status	Operation Type	Storage Policy	Job Type	Failed Folders	Failed Files	Start Time	End Time	Size of Application	Data Written	Savings Percentage	Move Snap to Media	U
130	Completed	Backup	Dedup Storage Policy	Full	0	0	2012/01/10 14:59:17	2012/01/10 15:12:55	4.48 GB	2.01 GB	55%	Not Applicable	a
131	Completed	Backup	Dedup Storage Policy	Full	0	0	2012/01/10 17:33:32	2012/01/10 17:46:48	4.48 GB	103.56 MB	97%	Not Applicable	a

Previous Next

Advanced - Deduplication to Disk

TABLE OF CONTENTS

License Requirements

DEDUPLICATION ARCHITECTURE

Deduplication provides a smart and efficient method to store data by identifying and eliminating the duplicate items in backups. When data is backed up for the first time, all the data is stored physically. If the same data is subsequently identified in another backup operation, then it is stored as a pointer to the previously stored copy.

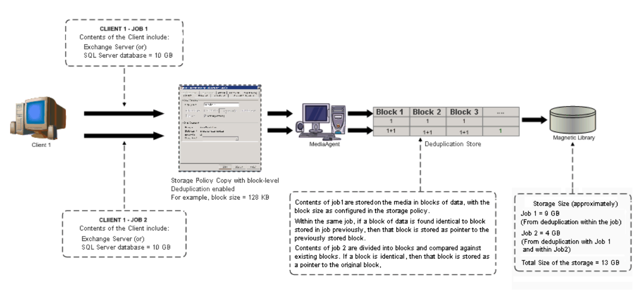
Deduplication is performed at the data block level by comparing blocks of data against each other. Block level deduplication allows you to deduplicate data within a given object. If an object (file, database, etc.) contains blocks of data that are identical to each other, then deduplication eliminates storing the redundant data and reduces the size of objects in storage.

Consider a backup containing data from Exchange Server or SQL Server database. Deduplication will divide the data into individual data blocks and then compare the different blocks against each other. If a data block is unique, then the block is stored on the media. If a data block is found to be identical to an existing block, then it is stored as a pointer to that block.

Identical data blocks within an object, as well as from objects within the same storage policy copy are deduplicated.

The diagram on the right illustrates the deduplication process.

The numbers in the diagram are meant for illustrative purposes. Additional space requirements (overheads) for storing metadata like File Access Control Lists will apply during actual deduplication enabled operations.



CLIENT 1 - JOB 1
Contents of the Client include:
Exchange Server (or)
SQL Server database = 10 GB
Client 1
CLIENT 1 - JOB 2
Contents of the Client include:
Exchange Server (or)
SQL Server database = 10 GB
Storage Policy Copy with block-level
Deduplication enabled
For example, block size = 128 KB
MediaAgent
Block 1
Block 2
Block 3
....
1
1
1
1+1
1+1
1+1
1
Deduplication Store
Magnetic Library
Contents of job1 are stored on the media in blocks of data, with the block size as configured in the storage policy.
Within the same job, if a block of data is found identical to block stored in job previously, then that block is stored as pointer to the previously stored block.
Contents of job 2 are divided into blocks and compared against existing blocks. If a block is identical, then that block is stored as a pointer to the original block,
Storage Size (approximately)
Job 1 = 9 GB
(From deduplication within the job)
Job 2 = 4 GB
(From deduplication with Job 1 and within Job2)
Total Size of the storage = 13 GB

Deduplication uses a hashing algorithm to compare data. A Signature Generation module computes the hashed signature for each block and then compares it with the existing signatures maintained in a Deduplication Store to determine whether it is identical. Based on the comparison, the MediaAgent performs one of the following operations:

- If the signature is unique, the data is stored and an entry added to the Deduplication Store for subsequent comparisons.
- If the signature is identical to an existing signature, additional entries are created in the Deduplication Store with pointers to the existing storage.

The deduplicated data are stored in specially designed container files to increase the system throughput and scalability.

HOW DOES DEDUPLICATION WORK

Deduplication is easy-to-use and does not require additional configurations once it is setup. The following table describes the various operations when deduplication is enabled.

OPERATION	DESCRIPTION
Backup Operations	The sequence of operations is almost similar to a regular backup job when deduplication is enabled. When a backup job is initiated the backup module secures the data and starts the data transfer module to the MediaAgent. The following sequence of events occur when data is secured: ● If data compression is enabled on the client, data is first compressed. ● Then, the signature generation module computes the signatures, if it is enabled on the client. ● Finally data is encrypted if client encryption is enabled.
Restore Operations	Data Recovery operations are identical to regular restore operations and are virtually unaffected by deduplication. Deduplication store is not contacted for normal restore operations, except when the data is not available in the disk. All types of restore operations (including Restore by Jobs and Restoring from copies) are supported.
Auxiliary Copy	Auxiliary Copy operations will automatically unravel or explode the deduplicated data, if deduplication is not enabled in the copy. If the secondary copy is set up for Deduplication, then a separate Deduplication Store gets created for the copy and the associated data is deduplicated for secondary copy.
Data Aging Operations	Data Aging operations will automatically look up the Deduplication Store before data is deleted from the disk. Data Aging will only delete the source data when all the references to a given block is pruned. So if you see older chunks in disk libraries remaining on the volume even if the original data is deleted, it might be due to the fact that valid deduplication reference(s) to the chunk exists within the data.
Data Encryption and Data Compression	When Data Encryption and/or Data Compression are enabled the system automatically runs the signature module after data compression and before data encryption. If the setup contradicts this order, the system will automatically perform compression, signature generation and encryption in the source client computer. When you have a primary copy that is encrypted (and is not deduplicated), enabling deduplication on a secondary copy will not accomplish any viable deduplication on the secondary copy. This is because each backup includes unique encryption keys which in turn will cause unique signatures for each backup. Deduplication does not support pass phrase protected data encryption.

Data Multiplexing	Data Multiplexing is not supported with Deduplication. Also a storage policy copy enabled for Deduplication cannot have a direct or indirect source copy enabled for Data Multiplexing. However an Auxiliary Copy can be configured with Data Multiplexing when the source copy is enabled for Deduplication.
Spool Copy	Deduplication-enabled Storage Policy Copies cannot be configured as Spool Copies. Note that existing deduplicated Spool Copies will continue to exist until the Spool Copy retention setting is removed; once removed, the deduplicated copy cannot be configured as a Spool Copy.
Deduplication Jobs on Migrated CommCell	After CommCell Migration, the Deduplication Store operates in the read-only mode in the destination CommCell. The migrated (deduplication enabled) storage policies in the destination CommCell can be used to restore the deduplicated data migrated from the source CommCell and to perform Auxiliary Copy operation with the migrated data as the source. Migrated Storage Policies in the destination CommCell cannot be used to deduplicate new backup operations.

DEDUPLICATION STORE

WHAT IS A DEDUPLICATION STORE

The Deduplication store (or the Deduplication Database) serves as the repository for signatures associated with all blocks that are backed up. It also has the reference counts to copies of the blocks that are backed up using the storage policy copy.

Deduplication stores are maintained for each Storage Policy Copy that has the deduplication option enabled. Multiple MediaAgents can be a part of the same copy and use the same Deduplication Store provided the libraries accessed by the MediaAgents are configured as static shared libraries and accessible from all the MediaAgents.

SUPPORTED PLATFORMS

The Deduplication Store is configured when creating a storage policy copy, both for primary and secondary storage policy copies. Any MediaAgent can be associated in the Deduplication Store.

The MediaAgent associated with data store could be any one of the MediaAgents in the data paths, or outside of the data path too. You can also change the MediaAgent hosting the Deduplication Store.

Deduplication store can be located on any of the following platforms:

Windows	All platforms supported by Windows MediaAgents, except 64-bit editions on Intel Itanium (IA64) and Windows XP. Supported on NTFS.
Linux	All platforms supported by Linux MediaAgents, except Power PC (Includes IBM System p). Supported on ext3 and ext4.
Microsoft Cluster Service (MSCS)	Clusters supported by Windows MediaAgents. Supported on NTFS.
Linux Cluster	Clusters supported by Linux MediaAgents. Supported on ext3 and ext4.

Never delete the Deduplication Store manually. The Deduplication Store facilitates the deduplication of backup jobs and data aging jobs. If deleted, new deduplicated backup jobs cannot be performed and the existing data in the disk mount paths will never be pruned.

DISK SPECIFICATIONS FOR HOSTING THE DEDUPLICATION STORE

To ensure optimal performance for deduplication operations, the disk hosting the Deduplication Store must satisfy the following specifications. Note that these specifications are only for the disk hosting the Deduplication Store, and not for the entire mount path.

- The Deduplication Store must be located on a fast access local disk with high throughput and superior disk protection.

  Ensure that the average read throughput of the disk is around 500 GB per hour, and the average write throughput of the disk is around 400GB per hour.

  Calculate the average read and write throughputs from multiple samples (between three and ten), for a FILECOUNT of 500.

  Use the steps described in Measuring the Disk Performance to measure the disk throughput.
- The Deduplication Store must be located on a local drive in the MediaAgent in which it resides.

  UNC path is not supported for Deduplication Store access.
- For SAN-attached configurations, it is desirable to have a dedicated channel on the HBA card to handle the input/output operations for the disk.
- ISCSI connections are not suited to the throughput requirements necessary to sustain high performance deduplicated data movement operations.
- Disk configuration specifications associated with the deduplication database LUN are as follows:
  - Disk LUN must be formatted to a block size of 4 KB.
  - A dedicated drive/set of drives must be provided for the deduplication database LUN.
  - Larger amounts of disk read/write cache enables increased throughput to the deduplication database.

- LUNs must be configured such that no more than 4 deduplication databases are configured on any one RAID group.
- Depending on the site tolerance for risk versus cost, RAID 0, 1, or 5 can be used for the RAID set. Also, stripe depth should be set to 8.

EVALUATING THE DISK FOR HOSTING DEDUPLICATION STORE

The following section provides information on how to evaluate the disk in which you plan to create the Deduplication Store. This will help you to determine the size of the data and store that can be hosted on the disk.

You can also use the user-interface version of this tool. See SIDB Simulator for more details and usage.

Running the Tool	Run the following file from the MediaAgent computer hosting the Deduplication Store. `C:/Program Files/`Bull Calypso/Calypso`/Base/SIDB2.exe`
Usage	`SIDB2 -simulateddb -p <SidbLocation> -in <Instance#> [-datasize] [-dratio] [-blocksize] [tlimit] [-diskperf -tpath] [-user] [-password] [-domain]` Where: Options in [] denotes optional arguments `-simulateddb` is the keyword to simulate the deduplication database to evaluate the disk compatibility for hosting the deduplication store. `-p` is the location (an empty directory) where the deduplication store will be located. `-in` is the instance of the software using the tool. `-datasize` is the application data size in GB. Number. `-dratio` is the expected deduplicaiton ratio. Number (default value is 5.) `-blocksize` is the deduplication data block size in KB. Number (default is 128.) `-tlimit` is the value in microsecond. Number (default value is 1000.) `-tlimit` and `-datasize` arguments cannot be used together. `-samplesize` is the size of the sample. Number (default values is 10000.) `-diskperf` and `-tpath`. Diskperf is the keyword to measure disk performance and tpath is the path of the disk. If you use `-diskperf`, `-tpath` is mandatory. `-keepddb` is the option to keep the deduplication database files. The files are removed by default. -stopCounter signifies how many additional iterations to process after reaching the threshold time. This is to limit spikes caused by caching. (default value is 50.)

Example 1	For the details on the projected average transaction time for an insert/query in the deduplication database based on the size of the application data that is backed up, use the tool with the `-simulateddb` and `-datasize` options.
	COMMAND
	`SIDB2 -simulateddb -in instance001 -p d:\dedup_store -datasize 500`
	SAMPLE OUTPUT
	`The disk is capable of hosting a deduplication DB for:`
	`0.500 TB of Application Data Size`
	`0.100 TB of data on disk`
	`146.0 microseconds average Q&I overhead perblock`
	`Throughput for DDb server 3156 GB per Hour`

Example 2	For recommendations on the maximum application data size that can be backed up using the store based on the average access time for each record, use the tool with the `-simulateddb`. This will run till it reaches the default threshold time limit of 1000 microseconds. **EXAMPLE** `SIDB2 -simulateddb -in instance001 -p d:\dedup_store`
Example 3	For recommendations on disk performance, use the tool with the `-simulateddb` and `-diskperf` options. **EXAMPLE** `SIDB2 -simulateddb -in instance001 -p d:\dedup_store -datasize 100 -diskperf -tpath d:\disktest`

MEASURING THE DEDUPLICATION DISK PERFORMANCE

Use the following steps to measure the disk throughput for the disk in which you plan to create the Deduplication Store.

Running the Tool	Run the following file from the MediaAgent computer hosting the Deduplication Store.
	Windows:
	`C:/Program Files/`Bull Calypso/Calypso`/Base/CvDiskPerf.exe`
	Linux:
	`./CVDiskPerf`

Usage

```
Windows:
CvDiskPerf -READWRITE -PATH <SIDB path> -RANDOM -FILECOUNT <filecount> -USER <username> -PASSWORD
<password> -DOMAIN <domain> -OUTFILE <outputfile>
```

Linux:

```
./CVDiskPerf -READWRITE -PATH <path> -RANDOM -FILECOUNT <filecount> -OUTFILE <outputfile>
```

Where:

`-READWRITE` is the option to measure read/write performance.

`-PATH` is the deduplication store mount path to be tested for performance.

`-RANDOM` is the keyword to measure random read/write operations (Optional). By default, sequential read/write operations are measured.

`-FILECOUNT` is the number of files used in the read and write operations (Optional). Default value is 1024.

`-USER, -PASSWORD, and -DOMAIN` are options to provide specific user credentials to impersonate access to the path provided in the `–PATH` option (Optional). By default, the application user-credential will be used. If domain name is not provided, then the default domain will be used.

`-OUTFILE` is the location of the output file to store the disk performance results (Optional). Default value is '.\CvDiskPerf.txt'

Sample Commands

Windows:

```
CvDiskPerf -READWRITE -PATH c:\SIDB01 -OUTFILE c:\temp\perf.txt
CvDiskPerf -READWRITE -RANDOM -PATH c:\SIDB01 -OUTFILE c:\temp\perf.txt
CvDiskPerf -READWRITE -RANDOM -PATH c:\SIDB01 -USER commuser –PASSWORD commpw -OUTFILE
c:\temp\perf.txt
```

Linux:

```
./CVDiskPerf -READWRITE -RANDOM -PATH /test1 -OUTFILE /tmp/CVDISKLIB01.log
```

Output

The details of the disk performance are stored in the output file provided in the `-OUTFILE` option. The contents of a sample output file are given below:

```
DiskPerf Version        : 1.3
Path Used               : f:\
Read-Write type         : RANDOM
Block Size              : 128
Block Count             : 1024
File Count              : 500
Total Bytes Written     : 1048576000
Time Taken to Write(S)  : 7.113515
Throughput Write(GB/H)  : 494.217709
Total Bytes Read        : 1048576000
Time Taken to Read(S)   : 7.581667
Throughput Read(GB/H)   : 463.700792
Time Taken to Create(S) : 1.16
Throughput Create(GB/H) : 325.04
```

Ensure that the average read throughput of the disk is around 500 GB per hour, and the average write throughput of the disk is around 400GB per hour.

Calculate the average read and write throughputs from multiple samples (between three and ten), for a FILECOUNT of 500.

The following table provides a sample of the disk performance calculation:

DISK PERFORMANCE	THROUGHPUT IN GB/HOUR	
	WRITE	READ
Sample 1	341.3798	477.6198
Sample 2	344.3546	513.2807
Sample 3	340.8644	575.6513
Sample 4	428.8675	499.7836
Sample 5	397.6285	426.5668
Sample 6	438.2224	503.0041
Sample 7	428.0591	494.4092
Sample 8	427.0613	643.4305

Sample 9	446.6219	523.7768
Sample 10	396.5592	581.3948
Average	**398.9619**	**523.8918**

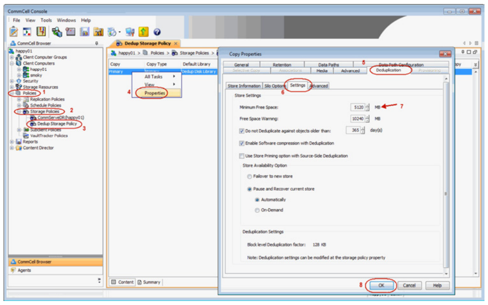
MANAGING THE DEDUPLICATION STORE

SETTING UP THE MINIMUM FREE SPACE

The minimum free space that must be available at all times in the volume in which the Deduplication Store is configured. By default, if the free space is less than 2GB on the volume hosting the Deduplication Store, jobs will not continue.

Use the following steps to set the minimum free space.

1. From the CommCell Browser, navigate to **Policies** | **Storage Policies** | ***<Storage_Policy>***.
2. Right-click the primary storage policy copy displayed in the right pane and click **Properties**.
3. Click the **Deduplication** tab, and then click the **Settings** tab.
4. In the **Minimum Free Space** box, type or select the amount of free space you want to change.
5. Click **OK**.



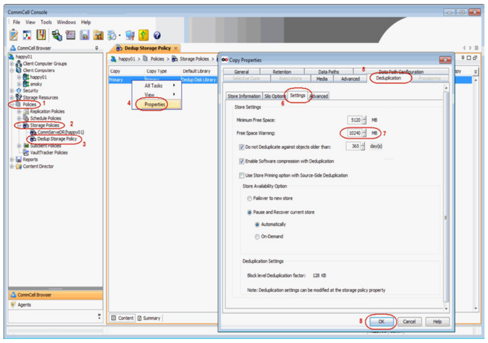
Store Settings
Minimum Free Space: 5120 MB
Free Space Warning: 10240 MB
☑ Do not Deduplicate against objects older than: 365 day(s)
☑ Enable Software compression with Deduplication
□ Use Store Priming option with Source-Side Deduplication
Store Availability Option
○ Failover to new store
● Pause and Recover current store
● Automatically
○ On-Demand
Deduplication Settings
Block level Deduplication factor: 128 KB
Note: Deduplication settings can be modified at the storage policy property

SETTING UP AN ALERT FOR FREE SPACE

If the amount of free space falls below the specified amount in the volume in which the Deduplication Store is stored, the MediaAgent generates an event message and generates the **MediaAgents (Disk Space Low)** alert, if configured.

Use the following steps to set the minimum free space to generate the alert:

1. From the CommCell Browser, navigate to **Policies** | **Storage Policies** | ***<Storage_Policy>***.
2. Right-click the primary storage policy copy displayed in the right pane and click **Properties**.
3. Click the **Deduplication** tab, and then click the **Settings** tab.
4. In the **Free Space Warning** box, type or select the amount of free space you want to change to generate alert.
5. Click **OK**.



Store Settings
Minimum Free Space: 5120 MB
Free Space Warning: 10240 MB
☑ Do not Deduplicate against objects older than: 365 day(s)
☑ Enable Software compression with Deduplication
□ Use Store Priming option with Source-Side Deduplication
Store Availability Option
○ Failover to new store
● Pause and Recover current store
● Automatically
○ On-Demand
Deduplication Settings
Block level Deduplication factor: 128 KB
Note: Deduplication settings can be modified at the storage policy property

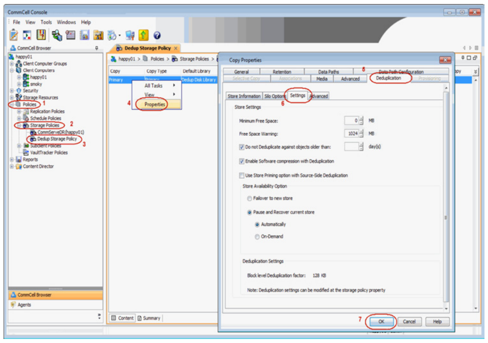
SETTING THE AGE OF THE PRIMARY BLOCK

You can set the number of days after which a block cannot be used for new deduplication. Setting this value will ensure that very old blocks are not allowed as the 'origin' data for newer backup jobs that are deduplicated.

Use the following steps to set the number of days after which a block cannot be used for deduplication:

1. From the CommCell Browser, navigate to **Policies** | **Storage Policies** | ***<Storage_Policy>***.
2. Right-click the primary storage policy copy displayed in the right pane and click **Properties**.
3. Click the **Deduplication** tab, and then click the **Settings** tab.
4. In the **Do not Deduplicate against objects older than** box, type or select the number of days you want to change for deduplication reference.

   If you do not specify the value, the default value is set to infinite.
5. Click **OK**.



Store Settings
Minimum Free Space: 0 MB
Free Space Warning: 1024 MB
☑ Do not Deduplicate against objects older than: day(s)
☑ Enable Software compression with Deduplication
□ Use Store Priming option with Source-Side Deduplication
Store Availability Option
○ Failover to new store
● Pause and Recover current store
● Automatically
○ On-Demand
Deduplication Settings
Block level Deduplication factor: 128 KB
Note: Deduplication settings can be modified at the storage policy property

SETTING UP DATA COMPRESSION

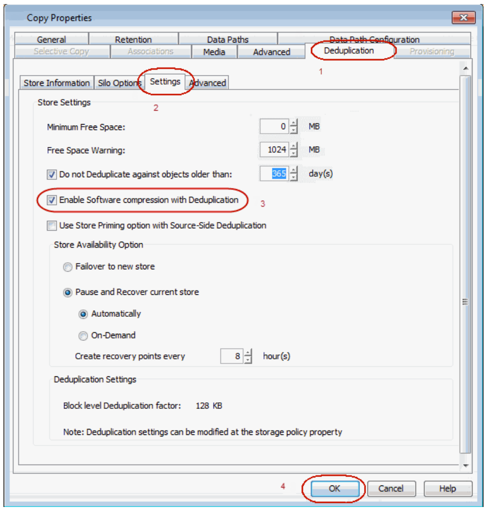
By default when deduplication storage policy is configured, compression is automatically enabled for the storage policy copy. This setting overrides the subclient compression settings by enabling **Use Storage Policy Settings** option at subclient level. For most of the data types the compression is recommended. This process works by compressing the blocks and then generating a signature hash on the compressed block.

Use the following steps to enable data compression for all subclients to storage policy:

1. From the CommCell Browser, navigate to **Policies** | **Storage Policies | *<Storage_Policy>***.
2. Right-click the primary storage policy copy displayed in the right pane and click **Properties**.
3. Click the **Deduplication** tab, and then click the **Settings** tab.
4. Select the **Enable Software Compression with Deduplication** box.

   This options is enabled by default. It is recommended to have data compression enabled when using deduplication.

   When this option is enabled the **Use Storage Policy Settings** option is enabled by default on the corresponding subclients.
5. Click **OK**.



Store Settings

Minimum Free Space: 0 MB

Free Space Warning: 1024 MB

☑ Do not Deduplicate against objects older than: 365 day(s)

☑ Enable Software compression with Deduplication

☐ Use Store Priming option with Source-Side Deduplication

Store Availability Option

○ Failover to new store

● Pause and Recover current store

● Automatically

○ On-Demand

Create recovery points every 8 hour(s)

Deduplication Settings

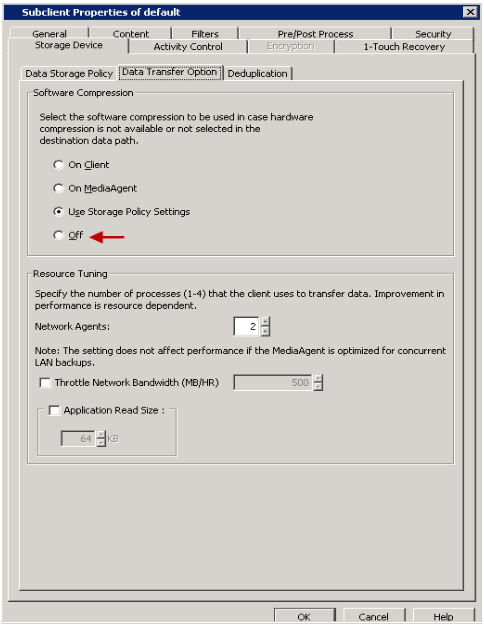
Block level Deduplication factor: 128 KB

Note: Deduplication settings can be modified at the storage policy property

MODIFY DATA COMPRESSION ON SPECIFIC SUBCLIENT

By default, all associated subclients uses the compression settings set on the deduplication storage policy copy. To modify or turn off the compression settings on the subclients, use the following steps:

1. From the CommCell Browser, navigate to **Client Computers** | ***<Client_Computer>* | File System | defaultBackupSet.**
2. Right-click the ***<Subclient>*** to which the deduplication storage policy is associated and then click **Properties**.
3. Click the **Storage Device** tab, and then click the **Data Transfer Option** tab.
4. In the **Software Compression** area, **Using Storage Policy Settings** option is selected by default.
   - Select **On Client** option to perform compression on client.
   - Select **On MediaAgent** option to perform compression on MediaAgent.
   - Select the **Off** option to turn off the compression.
5. Click **OK**.



Software Compression

Select the software compression to be used in case hardware compression is not available or not selected in the destination data path.

○ On Client

○ On MediaAgent

● Use Storage Policy Settings

○ Off

Resource Tuning

Specify the number of processes (1-4) that the client uses to transfer data. Improvement in performance is resource dependent.

Network Agents: 2

Note: The setting does not affect performance if the MediaAgent is optimized for concurrent LAN backups.

☐ Throttle Network Bandwidth (MB/HR) 500

☐ Application Read Size : 64 KB

CHANGING THE MEDIAAGENT HOSTING THE STORE

Perform the following to change the MediaAgent hosting the deduplication store:

1. Stop the Services
2. Copy the Deduplication Store Content
3. Change MediaAgent Hosting Deduplication Store
4. Start the Services

STOP THE SERVICES

Make sure that there are no SIDB.exe and SIDB2.exe process are running on the MediaAgent from which the SIDB currently resides. Use the following steps to confirm that no process are running:

For Windows:

1. Click the **Start** button on the Windows task bar and then click **All Programs**.
2. Navigate to **bull** | **Calypso** and click **Service Control Manager**.
3. Select **All Services** in **Services.**
4. Click **Stop** to stop all services.

For Linux:

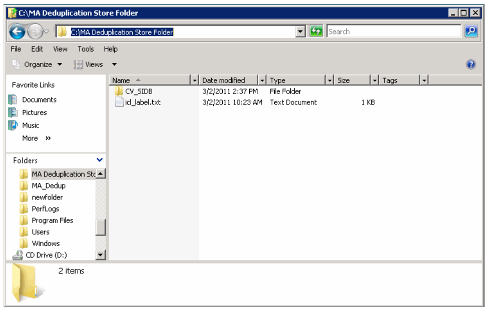
1. Log on to the computer as **root.**
2. Run the following command to stop services:

```
Calypso stop
```

COPY THE DEDUPLICATION STORE CONTENT

You need to manually copy the content available in the current Deduplication Store to the new mediaagent which you want to host the Deduplication Store. Use the following steps to copy the content available in the current Deduplication Store:

You cannot copy the deduplication database (SIDB) from Windows to Linux or from Linux to Windows location.



C:\MA Deduplication Store Folder

Name	Date modified	Type	Size	Tags
CV_SIDB	3/2/2011 2:37 PM	File Folder		
icl_label.txt	3/2/2011 10:23 AM	Text Document	1 KB	

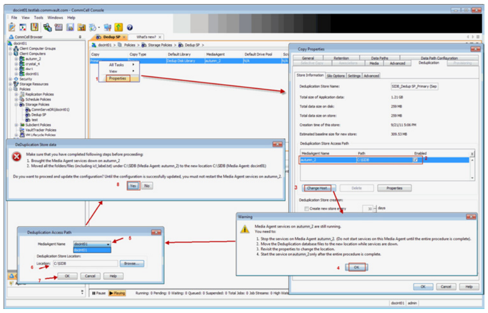
2 items

1. Login to the MediaAgent hosting the current Deduplication Store.
2. Navigate to the location where Deduplication database is available.
3. Copy the following available content on to a shared drive:
   - SIDB
   - icl_label.txt files
4. Login to the new MediaAgent that will be hosting a Deduplication Store.
5. From the share drive, copy the files into desired folder that will host the Deduplication Store.

   Make sure to note down the directory it is copied on.
6. Verify the size of the directory is in fact the same to ensure all data was copied.

CHANGE MEDIAAGENT HOSTING DEDUPLICATION STORE

Use the following steps to change the MediaAgent hosting the Deduplication Store:



DeDuplication Store data

Make sure that you have completed following steps before proceeding:
1. Brought the Media Agent services down on autumn_2
2. Moved all the folders/files (including icl_label.txt) under C:\SIDB (Media Agent: autumn_2) to the new location C:\SIDB (Media Agent: docint01)

Do you want to proceed and update the configuration? Until the configuration is successfully updated, you must not restart the Media Agent services on autumn_2.

Warning

Media Agent services on autumn_2 are still running.
You need to:
1. Stop the services on Media Agent autumn_2. (Do not start services on this Media Agent until the entire procedure is complete).
2. Move the Deduplication database files to the new location while services are down.
3. Revisit the properties to change the location.
4. Start the service on autumn_2 only after the entire procedure is complete.

Copy Properties

Deduplication Store Name: SIDB_Dedup SP_Primary (Sep
Total size of Application data: 1.21 GB
Total data size on disk: 259 MB
Total data size on store: 259 MB
Creation time of this store: 9/21/11 5:06 PM
Estimated baseline size for new store: 309.53 MB

MediaAgent Name	Path	Enabled
autumn_2	C:\SIDB	☑

Copy	Copy Type	Default Library	MediaAgent	Default Drive Pool
Primary		Dedup Disk Library	autumn_2	N/A

Deduplication Access Path

MediaAgent Name: docint01
Location: C:\SIDB

1. From the CommCell Browser, navigate to **Policies** | **Storage Policies** | ***<Storage_Policy>***.
2. Right-click the **Primary** copy displayed in the right pane and click **Properties**.
3. Click the **Deduplication** tab.
4. In the **Deduplication Storage Access Path** area, click **Change Host** button.
5. You will be prompted with a **Warning** message.

   If you have performed Stop the Services and Copy the Deduplication Store Content steps, then click **OK** and then click **Change Host** button.

   If you did not stop the services and did not copy the files, click **OK**, and then Stop the Services and Copy the Deduplication Store Content and then follow step 1.
6. From the **Deduplication Storage Access Path** dialog box, perform the following:
   - Select **<MediaAgent>** from **MediaAgent Name** drop-down list.
   - In the **Deduplication Store Location**, type the name of the folder to which the deduplication or click **Browse** button to select the folder in which the deduplication database must be located.

   The store information is displayed in the **Deduplication Store Access Path** area.
7. Click **OK**.

START THE SERVICES

If your old MediaAgent is in use hosting deduplication store for other storage policies and libraries or for backup, use the following steps to start the services.

For Windows:

1. Click the **Start** button on the Windows task bar and then click **All Programs**.
2. Navigate to **bull** | **Calypso** and click **Service Control Manager**.

3. Select **ALL Services** in **Services.**
4. Click **Start** to start all services.

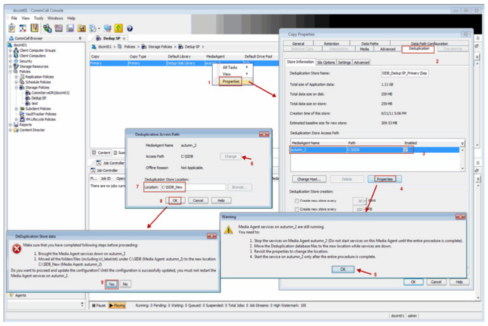
For Linux:

1. Log on to the computer as **root.**
2. Run the following command to start services:

```
Calypso start
```

CHANGING THE LOCATION OF THE DEDUPLICATION STORE

Use the following steps to change the location of the Deduplication Store in the existing MediaAgent:



Copy	Copy Type	Default Library	MediaAgent	Default Drive Pool
Primary	Primary	Dedup Disk Library	autumn_2	N/A

Deduplication Store Name: SIDB_Dedup SP_Primary (Sep

Total size of Application data: 1.21 GB

Total data size on disk: 259 MB

Total data size on store: 259 MB

Creation time of this store: 9/21/11 5:06 PM

Estimated baseline size for new store: 309.53 MB

Deduplication Store Access Path

MediaAgent Name	Path	Enabled
autumn_2	C:\SIDB	☑

Deduplication Store creation:

□ Create new store every 30 days

□ Create new store every 100 TB

There are no jobs curr

Deduplication Access Path

MediaAgent Name autumn_2

Access Path C:\SIDB

Offline Reason Not Applicable.

Deduplication Store Location:

Location: C:\SIDB_New

Warning

Media Agent services on autumn_2 are still running.
You need to:

1. Stop the services on Media Agent autumn_2 (Do not start services on this Media Agent until the entire procedure is complete).
2. Move the Deduplication database files to the new location while services are down.
3. Revisit the properties to change the location.
4. Start the service on autumn_2 only after the entire procedure is complete.

DeDuplication Store data

Make sure that you have completed following steps before proceeding:

1. Brought the Media Agent services down on autumn_2
2. Moved all the folders/files (including icl_label.txt) under C:\SIDB (Media Agent: autumn_2) to the new location C:\SIDB_New (Media Agent: autumn_2)

Do you want to proceed and update the configuration? Until the configuration is successfully updated, you must not restart the Media Agent services on autumn_2.

Running: 0 Pending: 0 Waiting: 0 Queued: 0 Suspended: 0 Total Jobs: 0 Job Streams: 0 High Watermark: 100

1. Make sure that no running jobs are currently accessing the store.
2. Stop the Services on existing MediaAgent by performing the following:

   For Windows:

   - Click the **Start** button on the Windows task bar and then click **All Programs**.
   - Navigate to **bull** | **Calypso** and click **Service Control Manager**.
   - Select **All Services** in **Services.**
   - Click **Stop** to stop all services.

   For Linux:

   - Log on to the computer as **root.**
   - Run the following command to stop services:

   ```
   Calypso stop
   ```

3. Copy the deduplication database files (SIDB, icl_label.txt files) to the new location.
4. From the CommCell Browser, navigate to **Policies** | **Storage Policies |** ***<Storage_Policy>***.
5. Right-click the **Primary** copy displayed in the right pane and click **Properties**.
6. Click the **Deduplication** tab.
7. In the **Deduplication Store Access Path** area, select ***<MediaAgent>*** and click the **Properties** button.
8. You will be prompted with a **Warning** message.

   If you have stopped the services and copied the store files to new location, then click **OK** and then click **Properties** button.

   If you did not stop the services and did not copy the files, click **OK**, and then follow from step 2.

9. In the **Deduplication Access Path** dialog, perform the following:
   - Click **Change** button.
   - In the **Deduplication Store Location** box, type the name of the folder in which the deduplication database must be located.
   - Click **OK**.
10. In the **Deduplication Store Data** dialog box, click **Yes,** if you have completed the steps provided in the dialog box.

    The store information will be displayed in the **Deduplication Store Access Path** area.

11. Click **OK**.
12. Start the services.

CONFIGURING DEDUPLICATION STORE CREATION

By default, a new Deduplication Store is created for every 100 TB of data. Note that this is the amount of data stored on the media after deduplication.

Use the following steps to create new Deduplication Store:

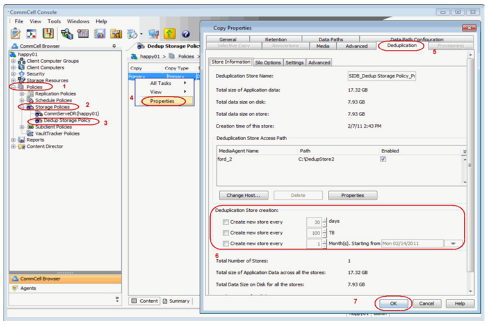
1. From the CommCell Browser, navigate to **Policies** | **Storage Policies |** ***<Storage_Policy>***.
2. Right-click the primary storage policy copy displayed in the right pane and click **Properties**.
3. Click the **Deduplication** tab.
4. In the **Deduplication Store Creation**, select one of the following:

- ○ Select **Create new store every - days** and specify the number of days after which a new Deduplication Store must be created.
- ○ Select **Create new store every - TB** and specify the size of the store, reaching which a new Deduplication Store must be created.

  If above both options are set, a new Deduplication Store will be created if either one of the two conditions is satisfied.

- ○ Select **Create new store every - Month(s). Starting from...** and specify the month and start date for a new Deduplication Store creation.

5. Click **OK**.



Copy Properties

Deduplication Store Name: SIDB_Dedup Storage Policy_Pr

Total size of Application data: 17.32 GB

Total data size on disk: 7.93 GB

Total data size on store: 7.93 GB

Creation time of this store: 2/7/11 2:43 PM

Deduplication Store Access Path

MediaAgent Name	Path	Enabled
ford_2	C:\DedupStore2	☑

Deduplication Store creation:

☐ Create new store every 30 days

☐ Create new store every 100 TB

☐ Create new store every 1 Month(s). Starting from Mon 02/14/2011

Total Number of Stores: 1

Total size of Application Data across all the stores: 17.32 GB

Total Data Size on Disk for all the stores: 7.93 GB

SEALING DEDUPLICATION STORE

The currently active Deduplication Store can be sealed on-demand.

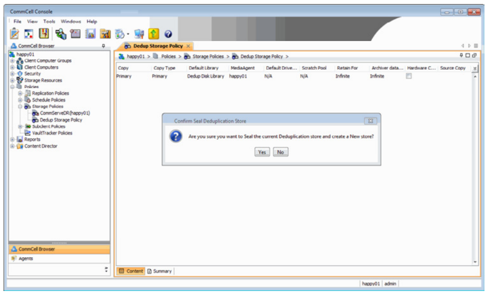
When a Deduplication Store is sealed:

- No new data is deduplicated in the store.
- The current Deduplication Store is closed.
- A new store is automatically created, and deduplication on new backup jobs is recorded in the new store.

The option to Seal Deduplication Stores is useful in rare cases when there are hardware issues or disk malfunction. Creating a new store will prevent new data from referencing any of the old data in the malfunctioned disks.

Use the following steps to seal the Deduplication Store:

1. From the CommCell Browser, navigate to **Policies** | **Storage Policies** | ***<Storage_Policy>***.
2. Right-click the primary storage policy copy displayed in the right pane, point to **All Tasks** and then click **Seal Deduplication Store**.
3. Click **Yes** on the **Confirm Seal Deduplication Store** dialog.



happy01 > Policies > Storage Policies > Dedup Storage Policy >

Copy	Copy Type	Default Library	MediaAgent	Default Drive...	Scratch Pool	Retain For	Archiver data...
Primary	Primary	Dedup Disk Library	happy01	N/A	N/A	Infinite	Infinite

Confirm Seal Deduplication Store

Are you sure you want to Seal the current Deduplication store and create a New store?

BACKING UP DEDUPLICATION DATABASE

Use the following method to backup the deduplication database so that it can be reconstructed in the unlikely event of an offline deduplication database. If this method is not used, the system will automatically use the automatic recovery process as described in Setting Up Automatic Recovery to reconstruct the database.

This is the recommended method of protecting the deduplication database. If there are multiple deduplication databases on the MediaAgent, this method automatically backs up all the deduplication databases.

This method performs a FULL backup of the deduplication database and the backup data is sent to the appropriate backup media based on the storage policy selected for the Deduplication Database subclient.

> If you have deduplication database hosted on Linux Intel Itanium (IA64) machine, deduplication database backups using DDB subclient is not supported. To backup deduplication databases, use automatic recovery process described in Setting Up Automatic Recovery.

FROM COMMCELL CONSOLE

Use the following steps to set up regular backup of deduplication database through CommCell Console:

CONFIGURE DDB SUBCLIENT

Use the following steps to create DDB subclient, assign storage policy to the subclient and then schedule the DDB backup.

1. File System *i*DataAgent must be installed on the MediaAgent hosting the deduplication store.

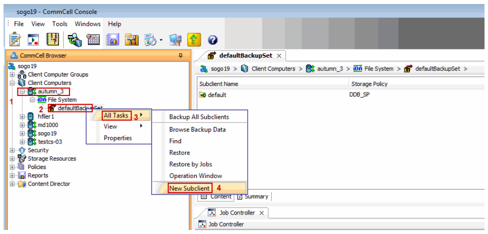
   You can install the File System *i*DataAgent as a **Restore Only Agent** without consuming any license.

   To do so, make sure to select **Install Agents for Restore Only** check box from the **Select Platforms** dialog box during File System *i*DataAgent installation.

   See Getting Started - Windows File System Deployment for step-by-step procedure.

2.

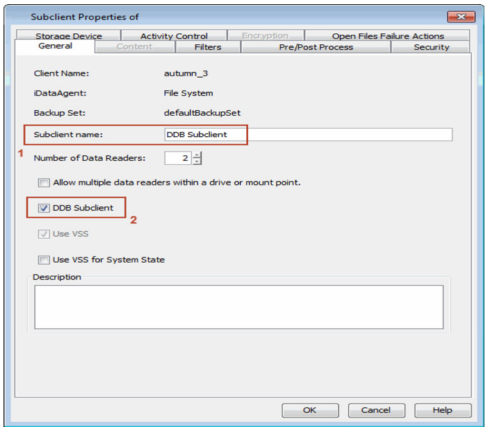
- From the CommCell Browser, navigate to **Client Computers | <MA_client_hosting_dedup_store> | File System**.
- Right-click the **defaultBackupSet**, point to **All Tasks** and then click **New Subclient**.



3.

- Type a name for the subclient in the **Subclient name**.
- Select the **DDB Subclient** check box.

DDB Subclient check box is available only when creating new subclients under defaultBackupSet.



Client Name: autumn_3

iDataAgent: File System

Backup Set: defaultBackupSet

Subclient name: DDB Subclient

Number of Data Readers: 2

□ Allow multiple data readers within a drive or mount point.

☑ DDB Subclient

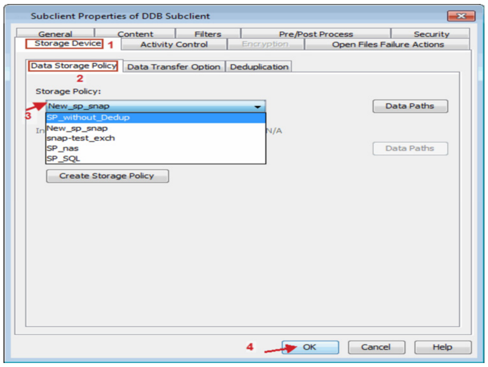
☑ Use VSS

□ Use VSS for System State

Description

4.

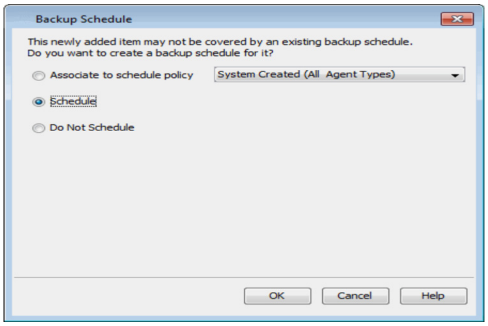
- Click the **Storage Device** tab.
- From the **Storage Policy** list, select a storage policy that does not have deduplication enabled for primary copy.
- Click **OK**.



Storage Policy: New_sp_snap

SP_without_Dedup
New_sp_snap
snap-test_exch
SP_nas
SP_SQL

5. Click **Schedule** and then click **OK.**



This newly added item may not be covered by an existing backup schedule.
Do you want to create a backup schedule for it?

○ Associate to schedule policy System Created (All Agent Types)

● Schedule

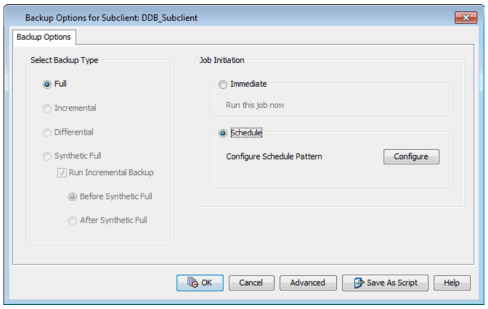
○ Do Not Schedule

6.

- From **Select Backup Type**, select **Full** option.

  Note that the other backup types such as incremental, differential etc., are not supported.

- From **Job Initiation**, select the **Schedule** option and then click **Configure**.



Select Backup Type

● Full

○ Incremental

○ Differential

○ Synthetic Full

☑ Run Incremental Backup

● Before Synthetic Full

○ After Synthetic Full

Job Initiation

○ Immediate

Run this job now

● Schedule

Configure Schedule Pattern

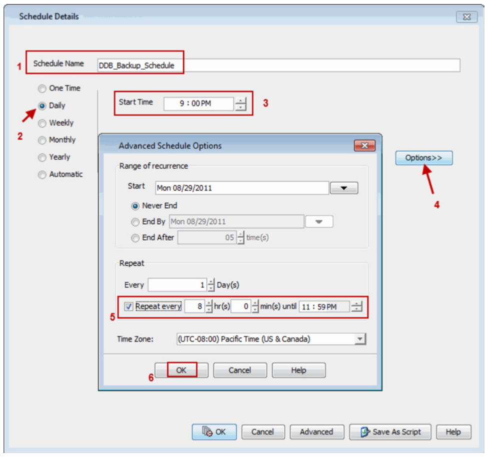
7.

- In the **Schedule Name** box, type a name of the schedule.
- Select the appropriate scheduling options.

For example, use the following steps to create a weekly schedule:

- Type a name for the schedule in the **Schedule Name** box.
- Select **Daily**.
- Type the **Start Time** to start the schedule.
- Click **Options >>** button.
- From the **Advanced Schedule Options** dialog box, select **Repeat** every check box.

  The default value is set to 8 hours.
- Click **OK**.



Schedule Details

1 Schedule Name: DDB_Backup_Schedule

2 ● Daily

3 Start Time: 9 : 00 PM

4 Options>>

Advanced Schedule Options

Range of recurrence

Start: Mon 08/29/2011

● Never End

○ End By: Mon 08/29/2011

○ End After: 05 time(s)

Repeat

Every: 1 Day(s)

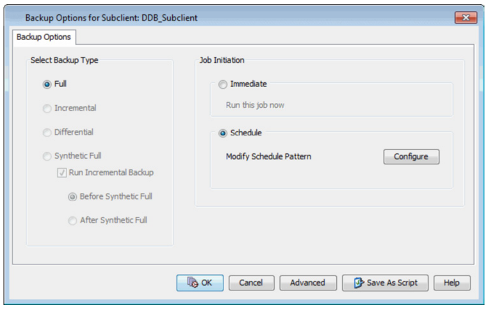
5 ☑ Repeat every 8 hr(s) 0 min(s) until 11 : 59 PM

Time Zone: (UTC-08:00) Pacific Time (US & Canada)

6 OK

8. Click **OK**.

   The new Deduplicate Database Store subclient will be displayed in the right-pane.



Backup Options for Subclient: DDB_Subclient

Backup Options

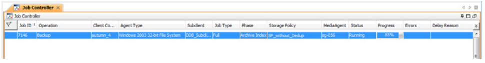
Select Backup Type: ● Full

Job Initiation: ● Schedule

Modify Schedule Pattern: Configure

9. When the schedule is run, the **Job Controller** window will display the backup job as shown in the sample image.

   During DDB backup job, if system detects reboot of a DDB MediaAgent, then the DDB backup job will go into **Pending** state. After reboot, the DDB backup job will restart from the beginning by creating a new snapshot of the DDB to perform the backup.



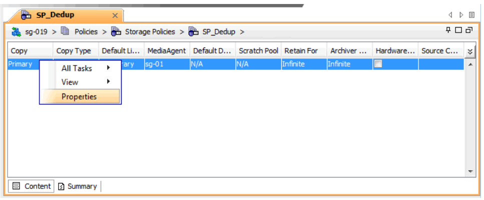
Job Controller

Job ID	Operation	Client Co...	Agent Type	Subclient	Job Type	Phase	Storage Policy	MediaAgent	Status	Progress	Errors	Delay Reason
7146	Backup	autumn_4	Windows 2003 32-bit File System	DDB_Subcl...	Full	Archive Index	SP_without_Dedup	sg-056	Running	85%		

SETTING UP AUTOMATIC RECOVERY

Use the following steps to set automatic recovery of a deduplication database.

10.
- From the CommCell Browser, navigate to **Policies** | **Storage Policies** | ***<Storage_Policy>*** where the deduplication store was created.
- Right-click the primary storage policy copy displayed in the right pane and click **Properties**.



SP_Dedup

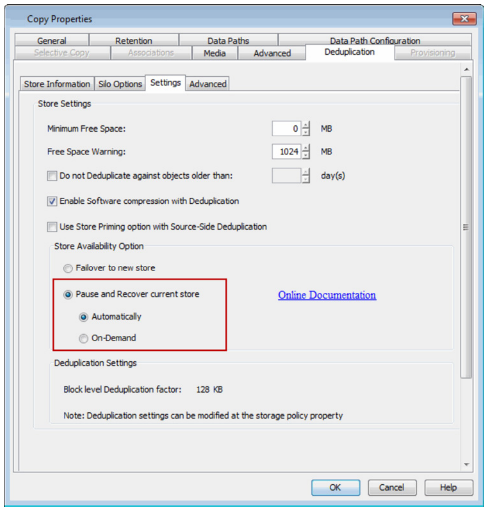
sg-019 > Policies > Storage Policies > SP_Dedup >

Copy	Copy Type	Default Li...	MediaAgent	Default D...	Scratch Pool	Retain For	Archiver ...	Hardware...	Source C...
Primary	...ary		sg-01	N/A	N/A	Infinite	Infinite	□	

11.
- Click the **Deduplication** tab, and then click the **Settings** tab.
- Ensure that **Pause and Recover current store** and **Automatically** options are selected.

  If you had **Failover to new store** selected, then make sure to Seal the Deduplication Database before selecting the **Pause and Recover current store** to prevent data loss.
- Click **OK**.

  After **DDB Subclient** creation and first successful backup of deduplication database store using DDB subclient, **Create recovery point every - Hour(s)** box will not be available.



Copy Properties

Store Settings

Minimum Free Space: 0 MB

Free Space Warning: 1024 MB

□ Do not Deduplicate against objects older than: day(s)

☑ Enable Software compression with Deduplication

□ Use Store Priming option with Source-Side Deduplication

Store Availability Option

○ Failover to new store

● Pause and Recover current store

● Automatically

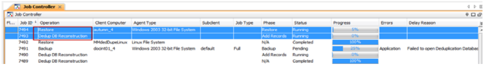
○ On-Demand

Deduplication Settings

Block level Deduplication factor: 128 KB

Note: Deduplication settings can be modified at the storage policy property

12. When the system detects a offline deduplication database, the **Job Controller** window will display the recover job as shown in the sample image.



Job Controller

Fl...	Job ID	Operation	Client Computer	Agent Type	Subclient	Job Type	Phase	Status	Progress	Errors	Delay Reason
	7494	Restore	autumn_4	Windows 2003 32-bit File System			Restore	Running	5%		
	7493	Dedup DB Reconstruction					Add Records	Running	0%		
	7492	Restore	MMdedDupeLinux	Linux File System			N/A	Completed	100%		
	7491	Backup	docint01_4	Windows 2003 32-bit File System	default	Full	Backup	Pending	25%	Application	Failed to open Deduplication Databas
	7490	Dedup DB Reconstruction					Add Records	Running	0%		
	7489	Dedup DB Reconstruction					N/A	Completed	100%		

FROM COMMAND LINE

Use the following steps to create DDB subclient through command line.

1. Open a XML editor, copy the sample XML parameter displayed on the right.
2. Provide a value for the following parameters:
   - *subclientName* - Name of the DDB subclient
   - *clientName* - Name of the MediaAgent on which you want to create the DDB subclient.

     Ensure that this MediaAgent has File System *i*DataAgent installed.
   - *storagePolicyName* - Name of the non-deduplicated storage policy which is used to backup the deduplication database.
3. Save the file as XML file. E.g., `ddbsubclient.xml`.
4. From Command prompt, navigate to `<Software_Installation_Directory>/Base` and then run the following command:
   - Login to the CommServe using the `qlogin` command and commcell credentials.

     For example, to log on to CommServe `server1` with username `user1`:

     ```
     C:\>qlogin -cs server1 - u user1
     ```
   - Run the XML using the `qoperation` command.

     For example, to run `ddbsubclient.xml`

     ```
     C:\>qoperation execute -af ddbsubclientxml
     ```
5. You can verify the DDB subclient from the MediaAgent client computer.
   - From the CommCell Brower, navigate to **Client Computers | *<MediaAgent>* | File System | defaultBackupSet**

     Newly created DDB Subclient will be displayed in right window.
   - Schedule the DDB backup to run for every 8 hours by performing the following:
     - Right click the newly created **DDB Subclient** and click **Backup.**
     - Click **Schedule** option.
     - Click **Configure** button.
     - Select **Daily**.
     - Type the **Start Time** to start the schedule.
     - Click **Options >>** button.
     - From the **Advanced Schedule Options** dialog box, select **Repeat** every check box.

       The default value is set to 8 hours.
     - Click **OK**.

SAMPLE XML PARAMETER

```
<?xml version="1.0"?>

<App_CreateSubClientRequest>

<subClientProperties contentOperationType="ADD">

<subClientEntity subclientName="DDBsubclient"
clientName="Name of the MediaAgent" appName="File
System"/>

<fsSubClientProp isDDBSubclient="true"/>

<commonProperties>

<storageDevice>

<dataBackupStoragePolicy storagePolicyName="Name of the
Storage Policy"/>

</storageDevice>

</commonProperties>

</subClientProperties>

</App_CreateSubClientRequest>
```

CONFIGURE ALERTS FOR DEDUPLICATION STORE BACKUP

Additionally, you can configure alert for deduplication store backup jobs to receive alerts when a deduplication store backup job fails and when there are no deduplication backup jobs.

Use the following steps to configure alert for the deduplication database backup:

1. From the CommCell Browser, click **Control Panel** and then double-click the **Email and IIS Configuration**.
2. In the **Mail Server** box, specify the mail server to be used by alerts. The **Mail Server** must support SMTP messages.
3. In the **Mail Server Port** box, select the port number.
4. In the **Mail Server Size** limit, specify the size limit per e-mail.
5. Click **OK**.
6. From the CommCell Browser, click **Control Panel** and then double-click the **Alerts**.
7. From the **Alert** dialog box, click **Add** button.
8. In the **Add Alert Wizard**, specify the following:
   - In the **Display Name** box, specify the name for the alert.

- In the **Category** list box, select **Job Management**.
- In the **Type** list box, select **Data Protection**.
- Click **Next**.
- From the **Entities Selection**, navigate to ***<client_computer>* | File System** and then select the ***<Deduplication_Backup_Subclient>*** and then click **Next**.

  If you have multiple deduplication backup subclients on multiple MediaAgent(s), select the ***<deduplication_backup_subclient>*** of each MediaAgent and then click **Next**.
- By default, **Job Failed** check box is selected which allows you to receive alerts when deduplication backup job fails.

  Select **No Data Protection** check box to receive alerts when there are no deduplication backup jobs.

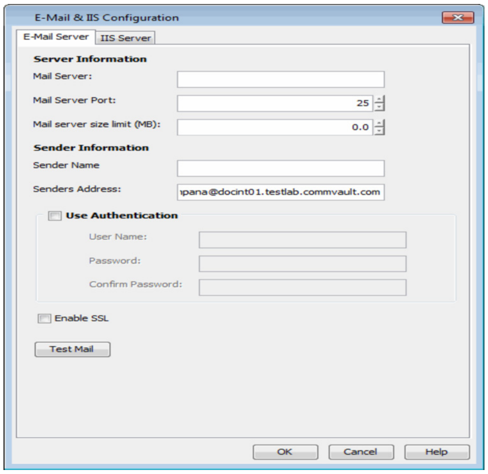
  Clear **Delayed by 1 Hrs** and **Job Succeeded with Errors** check boxes and then click **Next**.
- Select the way in which the alert is to be sent to its intended recipient. Select the **Select [Email/Pager] for notification** check box.

  If you wish to customize the e-mail or pager notification, click a token from the list and then click **Add Token**.
- Select the CommCell users and/or CommCell user groups that will receive the alert. Or,

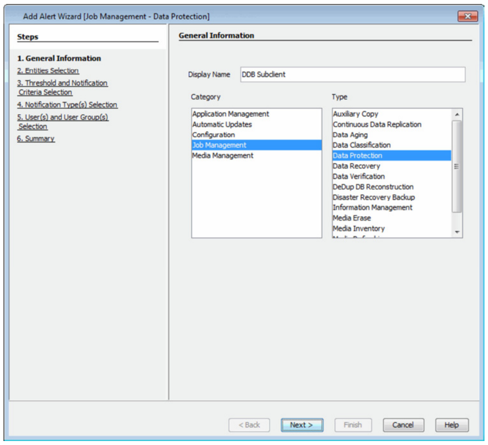
  Specify the e-mail address(es) of the recipient(s) in the **Email to Recipients** box, these recipients can reside within an external domain.

  Click **Next**.
- Verify the options you have selected for the alert in the **Summary** and then click **Finish**.

  The alert is now configured and displayed in the **Alerts** dialog box.
- Click **OK** to close the **Alerts** dialog box.



Mail Server:
Mail Server Port: 25
Mail server size limit (MB): 0.0
Sender Name
Senders Address: pana@docint01.testlab.commvault.com
□ Use Authentication
User Name:
Password:
Confirm Password:
□ Enable SSL


Add Alert Wizard [Job Management - Data Protection]
Steps
1. General Information
2. Entities Selection
3. Threshold and Notification Criteria Selection
4. Notification Type(s) Selection
5. User(s) and User Group(s) Selection
6. Summary
General Information
< Back
Next >
Finish
Cancel
Help

Display Name: DDB Subclient

Category: Application Management, Automatic Updates, Configuration, **Job Management**, Media Management

Type: Auxiliary Copy, Continuous Data Replication, Data Aging, Data Classification, **Data Protection**, Data Recovery, Data Verification, DeDup DB Reconstruction, Disaster Recovery Backup, Information Management, Media Erase, Media Inventory

DEDUPLICATION DATABASE RECOVERY

When the system detects an offline deduplication database (DDB), the DDB reconstruction job can be run to recover the DDB. During the deduplication database reconstruction job, the data in the DDB is validated against the CommServe database to ensure that both the databases are synchronized for successful recovery of the DDB. In addition, it allows you to use the same DDB in the future.

The following sections explain the different methods of recovering the deduplication database.

SETTING UP AUTOMATIC RECOVERY

When a system detects a offline deduplication store, the 'recover job' will automatically run to restore the deduplication store from the deduplication backup which was backed up using DDB subclient.

See Backing Up Deduplication Store Database for more information on backing up deduplication store.

Use the following steps to revert to the default settings if you have changed the store recovery points.

1. From the CommCell Browser, navigate to **Policies** | **Storage Policies | *<Storage_Policy>***.
2. Right-click the primary storage policy copy displayed in the right pane and click **Properties**.
3. Click the **Deduplication** tab, and then click the **Settings** tab.
4. Click **Pause and Recover current store**.
5. Click **Automatically**.

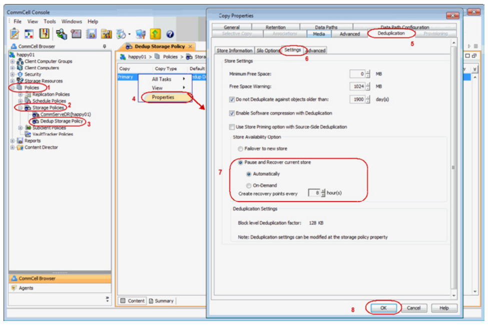
   If you had **Failover to new store** selected, then make sure to Seal the Deduplication Database before selecting the

Pause and Recover current store to prevent data loss.

6. In the **Create recovery points every - Hour(s)** box, type or change the frequency of Deduplication Store snapshots.

   You will be able to use the deduplication store snapshot frequency, if you have not already created a DDB subclient for backing up deduplication database.

7. Click **OK**.



Copy Properties — Deduplication — Settings

Store Settings

Minimum Free Space: 0 MB

Free Space Warning: 1024 MB

☑ Do not Deduplicate against objects older than: 1900 day(s)

☑ Enable Software compression with Deduplication

☐ Use Store Priming option with Source-Side Deduplication

Store Availability Option

○ Failover to new store

● Pause and Recover current store

● Automatically

○ On-Demand

Create recovery points every 8 hour(s)

Deduplication Settings

Block level Deduplication factor: 128 KB

Note: Deduplication settings can be modified at the storage policy property

MANUALLY RECONSTRUCTING A STORE

You can choose to recover from a offline deduplication store by manually reconstructing the store. If a offline deduplication store is detected, all jobs on that copy are paused until the store is manually reconstructed.

Use the following steps to configure and perform manual reconstruction:

SETTING UP MANUAL RECONSTRUCTION

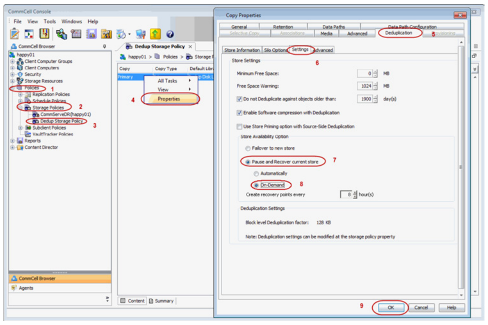
1. From the CommCell Browser, navigate to **Policies** | **Storage Policies** | ***<Storage_Policy>***.
2. Right-click the primary storage policy copy displayed in the right pane and click **Properties**.
3. Click the **Deduplication** tab, and then click the **Settings** tab.
4. Click **Pause and Recover current store** and then click **On-Demand**.

   If you had **Failover to new store** selected, then make sure to Seal the Deduplication Database before selecting the **Pause and Recover current store** to prevent data loss.

5. In the **Create recovery points every - Hour(s)** box, type or select the frequency of Deduplication Store snapshots.

   You will be able to use the deduplication store snapshot frequency, if you have not already created a DDB subclient for backing up deduplication database.

6. Click **OK**.



Copy Properties — Deduplication — Settings

Store Settings

Minimum Free Space: 0 MB

Free Space Warning: 1024 MB

☑ Do not Deduplicate against objects older than: 1900 day(s)

☑ Enable Software compression with Deduplication

☐ Use Store Priming option with Source-Side Deduplication

Store Availability Option

○ Failover to new store

● Pause and Recover current store

○ Automatically

● On-Demand

Create recovery points every 8 hour(s)

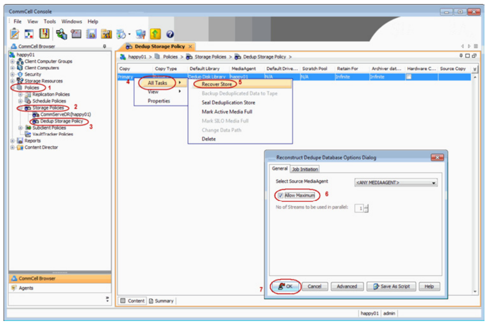
Deduplication Settings

Block level Deduplication factor: 128 KB

Note: Deduplication settings can be modified at the storage policy property

MANUALLY RECONSTRUCT A STORE

1. From the CommCell Browser, navigate to **Policies** | **Storage Policies** | ***<Storage_Policy>***.
2. Right-click the primary storage policy copy displayed in the right pane, point to **All Tasks** and then click **Recover Store**.
3. From the Select Source MediaAgent list, select MediaAgent from which you will run the reconstruct of the deduplication store database.
4. Select **Allow Maximum** check box.
5. Click **OK**.



Reconstruct Dedupe Database Options Dialog — General

Select Source MediaAgent: <ANY MEDIAAGENT>

☑ Allow Maximum

No of Streams to be used in parallel: 1

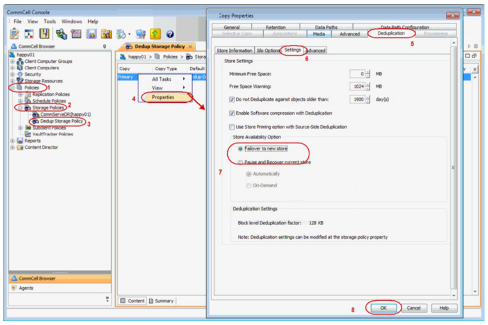
DEDUPLICATION STORE FAILOVER

You can choose to automatically create a new Deduplication Store in the event the active store becomes offline and deduplication database backup is not available. When configured, if a offline store is detected then the store is automatically sealed and a new store is created.

Use the following steps to automatically create a new Deduplication Store when the store becomes offline and deduplication database backup is not available:

1. From the CommCell Browser, navigate to **Policies** | **Storage Policies** | ***<Storage_Policy>***.
2. Right-click the primary storage policy copy displayed in the right pane and click **Properties**.
3. Click the **Deduplication** tab, and then click the **Settings** tab.

4. By default, **Failover to New Store** option is selected.
5. Click **OK**.



Variable Content Alignment

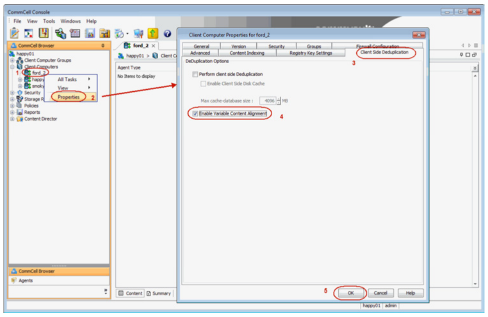
Variable content alignment is a content aware approach to deduplication that further reduces the amount of data stored during a database agents backup. It accomplishes this by aligning the segment boundaries of the backup data stream as minor changes to the data in the stream that are made between incremental backups. Therefore, the effectiveness of deduplication increases more with this feature on client systems that experience small changes to the backup data.

Variable content alignment is performed on the client system and consequently you may experience some performance overhead, especially when used together with software compression. You can enable variable content alignment as follows:

1. From the CommCell Browser, right-click the ***<Client>*** you wish to enable variable content alignment and then click **Properties**.
2. Click **Client Side Deduplication** tab.
3. Select **Enable Variable Content Alignment** check box.

   Enabling this option will consume more disk space. This happens because a fresh copy of the deduplicated data blocks with new signature is created for that deduplication database. Hence, this new signature will not match the existing signatures available in the deduplication database and thus creates a new baseline for the deduplication database.

4. Click **OK**.

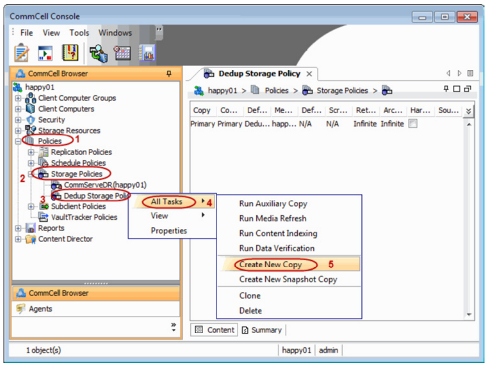

CommCell Console
Client Computer Properties for ford_2
Client Side Deduplication
Deduplication Options
Enable Variable Content Alignment
All Tasks
View
Properties
OK
Cancel
Help

Enabling Deduplication in Secondary Copies

Deduplication can be enabled for secondary copies during Storage Policy Copy creation. Once the copy is created, deduplication cannot be enabled later.

1.

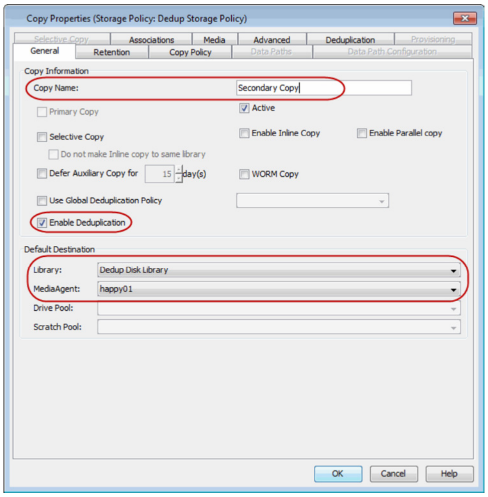
- From the CommCell Browser, navigate to **Policies** | **Storage Policies |** ***<Storage_Policy>***.
- Right-click ***<storage_policy>***, point to **All Tasks** and then click **Create New Copy**.



2.

- Specify name in **Copy Name**.
- From the **Library** list, click the name of a disk library.
- From the **MediaAgent** list, click the name of a MediaAgent.
- Select **Enable Deduplication** box. The **Deduplication** tab is enabled.
- Click **Deduplication** tab.

  Deduplication can only be enabled for storage policy copies associated with a disk library.



Copy Information

Copy Name: Secondary Copy

□ Primary Copy ☑ Active

□ Selective Copy □ Enable Inline Copy □ Enable Parallel copy

□ Do not make Inline copy to same library

□ Defer Auxiliary Copy for 15 day(s) □ WORM Copy

□ Use Global Deduplication Policy

☑ Enable Deduplication

Default Destination

Library: Dedup Disk Library

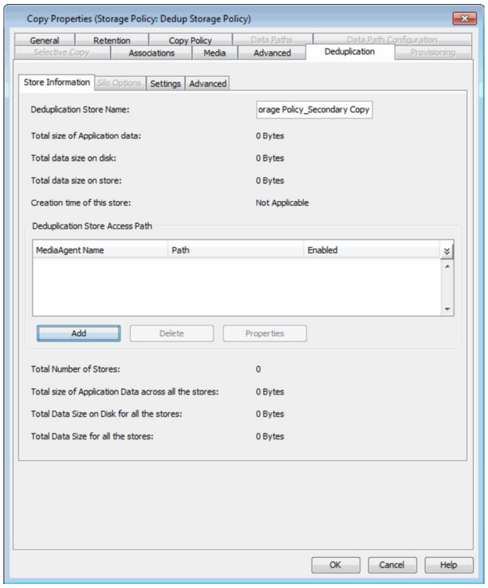
MediaAgent: happy01

Drive Pool:

Scratch Pool:

3.

- The default name of the deduplication store is displayed in **Deduplication Store Name** box.
- In the **Deduplication Store Access Path** area, click **Add.**



Deduplication Store Name: orage Policy_Secondary Copy

Total size of Application data: 0 Bytes

Total data size on disk: 0 Bytes

Total data size on store: 0 Bytes

Creation time of this store: Not Applicable

Deduplication Store Access Path

MediaAgent Name	Path	Enabled

Total Number of Stores: 0

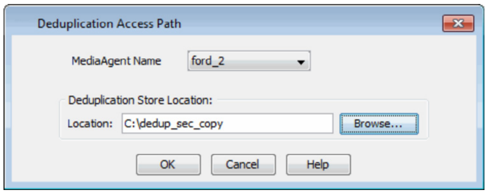
Total size of Application Data across all the stores: 0 Bytes

Total Data Size on Disk for all the stores: 0 Bytes

Total Data Size for all the stores: 0 Bytes

4.

- From the **MediaAgent** list, click the name of a MediaAgent.
- Type the name of the folder in which the deduplication database must be located in the **Deduplication Store Location** or click the **Browse** button to select the folder.
- Click **OK**.



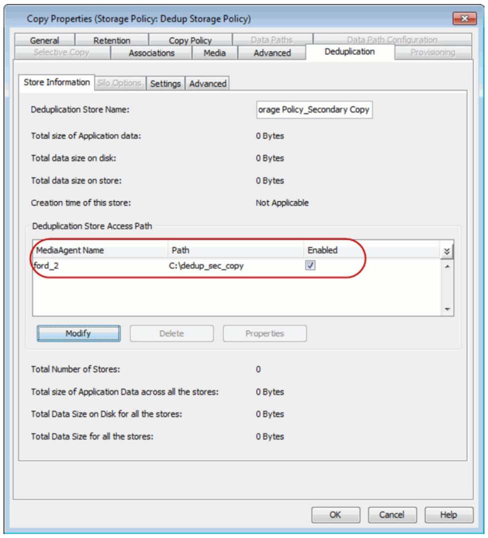
MediaAgent Name: ford_2

Deduplication Store Location:

Location: C:\dedup_sec_copy

5.

- The store information is displayed in the **Deduplication Store Access Path** area.
- Click **OK**.



Deduplication Store Name: orage Policy_Secondary Copy

Total size of Application data: 0 Bytes

Total data size on disk: 0 Bytes

Total data size on store: 0 Bytes

Creation time of this store: Not Applicable

Deduplication Store Access Path

MediaAgent Name	Path	Enabled
ford_2	C:\dedup_sec_copy	☑

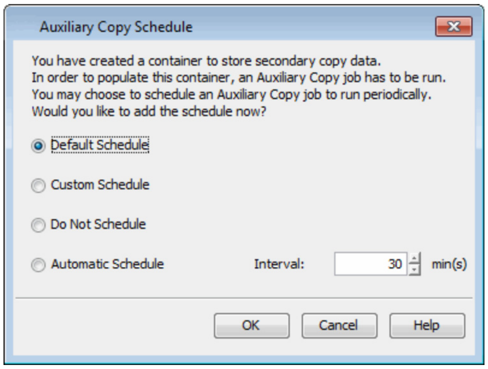
Total Number of Stores: 0

Total size of Application Data across all the stores: 0 Bytes

Total Data Size on Disk for all the stores: 0 Bytes

Total Data Size for all the stores: 0 Bytes

6. Click **OK** to accept the default schedule.



You have created a container to store secondary copy data.
In order to populate this container, an Auxiliary Copy job has to be run.
You may choose to schedule an Auxiliary Copy job to run periodically.
Would you like to add the schedule now?

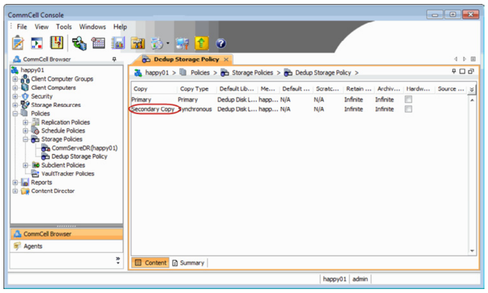
● Default Schedule

○ Custom Schedule

○ Do Not Schedule

○ Automatic Schedule Interval: 30 min(s)

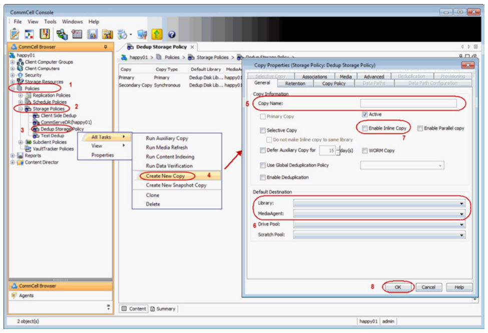
7. Secondary Copy is displayed in the **Storage Policy** pane.



Copy	Copy Type	Default Lib...	Me...	Default ...	Scrat...	Retain ...	Archiv...	Hardw...	Source ...
Primary	Primary	Dedup Disk L...	happ...	N/A	N/A	Infinite	Infinite	□	
Secondary Copy	Synchronous	Dedup Disk L...	happ...	N/A	N/A	Infinite	Infinite	□	

Enabling Inline Copy for Deduplicated Primary Copy

When the Primary Copy is deduplicated, you might want to create additional copies for offline storage. Note that you could use the auxiliary copy feature for this. But to create an Auxiliary Copy you would have to wait until the primary copy becomes available. This could cause delays in getting the data offsite. The Inline Copy feature allows you to create additional copies of data at the time of backups. Since the Primary Copy is the source for the Inline Copy the Inline Copy can be created along with the Primary Copy. However, note that the Inline Copy does not get deduplicated.



1. From the CommCell Browser, navigate to **Policies** | **Storage Policies** | ***<Storage_Policy>***.
2. Right-click ***<storage_policy>***, point to **All Tasks** and then click **Create New Copy**.
3. Specify name in the **Copy Name**.
4. From the **Library** list, click the name of a disk library.
5. From the **MediaAgent** list, click the name of a MediaAgent.

   Note that the MediaAgent must be the same as the Primary Copy.
6. Select **Enable Inline Copy** box.
7. Click **OK**.
8. In the **Auxiliary Copy Schedule**, click **OK** to accept the default schedule.

9. The **Inline Copy** created along with the Primary Copy will be displayed in the right-pane.

SETTING UP DEDUPLICATION FOR EXISTING NON-DEDUPLICATED DATA

Use the following steps to enable deduplication for existing non-deduplicated backup data.

1. Create a Storage Policy Copy with deduplication enabled. See Getting Started - Setup Deduplication for step-by-step instructions.
2. Create a Secondary Copy and run an auxiliary copy in the secondary copy. See Enabling Deduplication in Secondary Copies for step-by-step instructions.

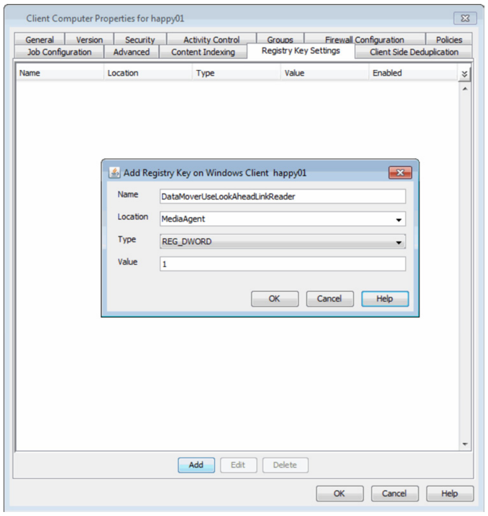
   If necessary you can promote the secondary copy as the primary copy so that subsequent backups are automatically deduplicated.

LOOK-AHEAD READER

To reduce the time taken to read the data during restore and auxiliary copy operations, deduplication-enabled operations can be performed using look-ahead reader. Use the following steps to enable the look ahead reader, by creating DataMoverUseLookAheadLinkReader registry key on the MediaAgent where the disk library is created.

Look-Ahead Reader operation is not applicable for Cloud Storage Library.

1. From the CommCell Browser, navigate to **Client Computers**.
2. Right-click the ***<Client>*** where the disk library attached to the primary storage policy copy is created and then click **Properties**.
3. Click the **Registry Key Settings** tab.
4. Click **Add**.
5. In the **Add Registry Key** dialog box, enter the following:
   - In the **Name** box, type **DataMoverUseLookAheadLinkReader** key.
   - In the **Location** list, click **MediaAgent**.
   - In the **Type** list, click **REG_DWORD**.
   - In the **Value** box, type **1**.
   - Click **OK**.
6. Click **OK**.



Name: DataMoverUseLookAheadLinkReader
Location: MediaAgent
Type: REG_DWORD
Value: 1

CONFIGURING SIGNATURE GENERATION

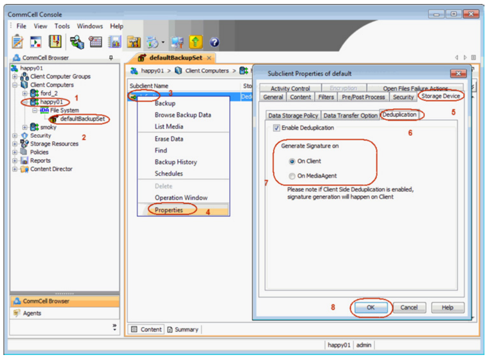
The signature generation module generates signatures for each block. This is done using SHA 512 (Secure Hash Algorithm) along with the size of the data. This combination eliminates the possibility of collisions, where two blocks hash to the same value.

The signature generation module can be configured either on the Client or the MediaAgent. Note that it is recommended to be run on the Client as it is both memory and resource intensive. Follow the steps described below to configure the signature generation:

1. Do not modify the properties of a subclient when a backup job associated with the subclient is in progress.
2. From the CommCell Browser, navigate to **Client Computers** | ***<Client>*** | **File System** | **defaultBackupSet**.
3. Right click the subclient for which you wish to enable (or disable) deduplication and click **Properties**.
4. Click the **Storage Device** tab and then click the **Deduplication** tab.
5. Select one of the following options for signature generation.
   - **On Client** option to enable the signature generation for Deduplication on the client computer.
   - **On MediaAgent** option to enable the signature generation for deduplication on the MediaAgent computer.

   By default, signature generation is set **On Client**.

The signature generation is performed only if the subclient is associated with a storage policy copy that is deduplication enabled.



☑ Enable Deduplication

Generate Signature on
● On Client
○ On MediaAgent

Please note if Client Side Deduplication is enabled, signature generation will happen on Client

6. Click **OK**.

DATA AGING

Data Aging operations will automatically look up the deduplication store before data is deleted from the disk. Data Aging will only delete the source data when all the references to a given block is aged. So if you see older chunks in disk libraries remaining on the volume even if the original data is deleted, it might be due to the fact that deduplication reference(s) to the chunk is still valid.

If a deduplication store is offline, then that store will not be aged until all data on the store is eligible for aging.

Do not manually delete the Deduplication Store. The Deduplication Store facilitates the deduplication backup jobs and data aging jobs. If deleted, new deduplicated backup jobs cannot be performed and the existing data in the disk mount paths will never be aged.

DISABLING DEDUPLICATION

Once enabled, deduplication cannot be disabled on a storage policy copy. However, you can use the following workaround to disable deduplication:

- Disable deduplication on all the subclients associated with the storage policy copy.
- Create a new storage policy without enabling Deduplication and re-point the necessary subclients to that storage policy.
- Create a secondary copy, and run an auxiliary copy in the secondary copy. Then promote the secondary copy as the primary copy.

SUSPENDING/RESUMING DEDUPLICATION

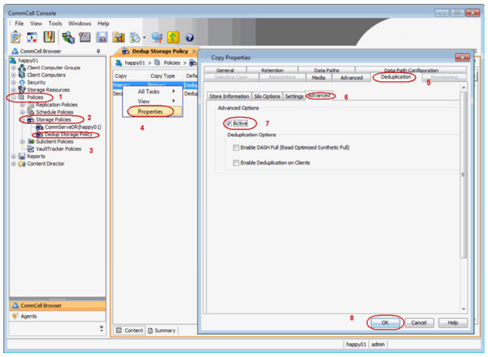
Although deduplication cannot be disabled, it can be temporarily suspended. Suspend deduplication to temporarily detach the Deduplication Store to gain access to the store, for diagnostics and maintenance purposes. Once you resume deduplication, the signature verification and data deduplication is resumed.

Follow the step-by-step instructions described below to suspend/resume:

1. From the CommCell Browser, navigate to **Policies** | **Storage Policies** | ***<Storage_Policy>***.
2. Right-click the primary storage policy copy displayed in the right pane and click **Properties**.
3. Click **Deduplication** tab, and then click the **Settings** tab.
4. In **Advanced Options** area, clear **Active** box to temporarily suspend deduplication.

   When a storage copy is deduplicated, this option is enabled by default.

   Select **Active** box to resume deduplication.
5. Click **OK**.



REBOOTING A MEDIAAGENT HOSTING THE DEDUPLICATION STORE

You may want to reboot a MediaAgent for installing updates or maintenance purposes. For MediaAgents controlling the deduplication database, you will have to ensure that all the deduplication transactions in the memory are completed before rebooting. Failure to follow the recommendations might result in the sealing of the Deduplication Store, which will increase the amount of storage space consumed in the primary disk library.

REBOOT A WINDOWS MEDIAAGENT

1. Click the **Start** button on the Windows task bar and then click **All Programs**.
2. Navigate to **bull** | **Calypso** and click **Service Control Manager**.
3. Select **All Services** in **Services.**
4. Click **Stop**.
5. When the services are stopped, open the Windows **Task Manager**.
6. Select the **Processes** tab and locate the `SIDB.exe` or `SIDB2.exe` process. If either of the processes is located, then wait until the process is complete.

   Depending on the size of the Deduplication database, this process might take as long as 30 minutes to complete.
7. Once the process is complete and no longer displayed on the task manager, reboot the computer.

REBOOT A UNIX MEDIAAGENT

1. Log on to the computer as **root** and run the following command to stop services:

   ```
   Calypso stop
   ```

2. When the services are stopped, type the following command to view all the deduplication processes that are still running.

   ```
   ps –aef | grep sidb
   ```

3. If either the `SIDB.exe` or `SIDB2.exe` process is found running, then wait until the process is complete.

   Depending on the size of the Deduplication database, this process might take as long as 30 minutes to complete.

4. Repeat **Step 2** to confirm that the processes are no longer running and then reboot the computer.

GRACEFUL SHUTDOWN OF MEDIAAGENT HOSTING THE DEDUPLICATION DATABASE

When a MediaAgent hosting the deduplication database (DDB) attempts to reboot or power off, by default the system doesn't halt and the operating system will shut down regardless of any processes that are running.

However, SIDB process has a built-in capability to receive the shutdown notification and to bring down the deduplication database gracefully if there is enough amount of time between the shutdown notification and the actual machine shutdown. In case where the graceful stopping of the DDB takes more time than the OS allows, it may still damage the DDB. In order to prevent the shutdown while the SIDB process is still running, the following method is suggested, which will prevent the shutdown in most of the cases.

To allow system to shut down gracefully when SIDB process is running, perform the following on Windows computer.

For Linux, the `Calypso stop` automatically handles the graceful shutdown of the MediaAgent.

Note that when MediaAgent attempts to reboot or shut down, the existing CVD process attempts to stop so that it do not accept any more requests. By setting up the below script, if there are any SIDB process that are running at this period, the CVD process will go into Stopping state and wait for SIDB process to gracefully exit before shutting down.

1. Install the latest version of Service Pack on the MediaAgent.

   This installs Update 34948 which automatically executes the **AddScripttoShutdownGPO.exe** script. This script allows the system to delay the reboot or shutdown till it reaches the grace period.

2. You can verify the **AddScripttoShutdownGPO.exe** script was executed successfully by performing the following:

   a. Logon to computer where the deduplication database is hosted.

   b. Click **Start**, click **Run...**, type **gpedit.msc**, and then click **OK**.

   c. From the **Local Group Policy Editor** window, navigate to **Local Computer Policy | Computer Configuration | Windows Settings | Scripts (Startup/Shutdown)**.

   d. In the right pane, double-click the **Shutdown** option.

   e. In the **Shutdown Properties** dialog box, **StopProc.vbs** script will be displayed.

      If **StopProc.vbs** script is not populated then perform the following:

      From the Command Prompt, navigate to the following location:

      ```
      <Installation Directory>\Base
      ```

      Run the following command:

      ```
      AddScripttoShutdownGPO.exe -vm InstanceXXX
      ```

      Repeat **step 2** to verify that the **StopProc.vbs** script is populated in the **Shutdown Properties**.

   f. Navigate to **Local Computer Policy | Computer Configuration | Administrative Templates | System | Scripts**

   g. In the right pane double click the **Maximum wait time for Group Policy** scripts.

   h. In the **Maximum wait time for Group Policy script Properties** dialog box, specify **1800** seconds (30 minutes). By default time is set to 600 seconds (10 minutes).

This waiting time prevents the shutdown while the SIDB process is running, allows the process to stop gracefully and not to damage the deduplication database.

To uninstall the script perform the following:

1. From the Command Prompt, navigate to the following location:

   ```
   <Installation Directory>\Base
   ```

2. Run the following command:

   ```
   AddScripttoShutdownGPO.exe -vm InstanceXXX -uninstall
   ```

   Once you run the above command, you will not see any delay in rebooting of your machine.

RELATED REPORTS

RECONSTRUCT DEDUPLICATION DATABASE JOB SUMMARY REPORT

When a Deduplication Store is offline, the Deduplication Store is automatically reconstructed based on the Deduplication Store availability options. This Reconstruct Deduplication Database report provides the information about the storage policy, Deduplication Store name to which it was reconstructed and status of the restore job.

The following procedure provides the steps necessary to run a Reconstruct Deduplication Database report:

1. From the CommCell Browser, click **Tools -> Reports...**
2. From the **Reports** pane, click **Job Summary**.
3. From the **General** tab, click **Administrative Jobs** and **Reconstruct Dedupe Database**.
4. Click **Run**.

STORAGE POLICY REPORT

The Storage Policy report provides deduplication related information including deduplication properties and Deduplication Store information. The following procedure provides the steps necessary to run Storage Policy report:

1. From the CommCell Browser, click **Tools -> Reports...**
2. From the **Reports** pane, navigate to **Storage** and click **Storage Policy**.
3. From the **General** tab, clear **Include All Storage Policies**.
4. Press **Ctrl** key and select ***<Storage_Policies>.***
5. Click **Include** to move the selected storage policies to the **Include** list box.
6. Select **Include Media** checkbox.
7. Click **Run**.

DISK USAGE

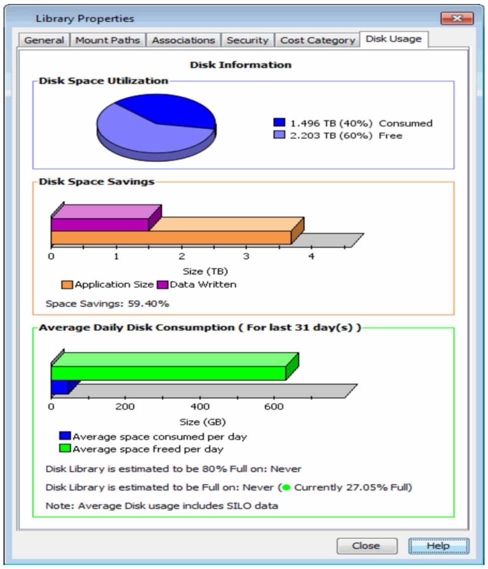
The disk usage report provides the following information:

- Total capacity available in the library
- Disk Space savings using deduplication
- Amount of space consumed and freed within the library over a period of time

Use the following steps to run the Disk Usage report:

1. From the CommCell Browser, navigate to **Storage Resources** | **Libraries**.
2. Right-click the **<Library>** and then click **Properties**.
3. Click the **Disk Usage** tab.

   The report will be displayed.



Space Savings: 59.40%

Disk Library is estimated to be 80% Full on: Never

Disk Library is estimated to be Full on: Never (● Currently 27.05% Full)

Note: Average Disk usage includes SILO data

LICENSE REQUIREMENTS

Deduplication requires following licenses based on the License Type:

- For Traditional License, **Block Level Deduplication** license is required.
- For License Usage by Capacity, **Data Protection Enterprise** (for Backup) or **Archive Enterprise** (for Archive) license is required.

Back to Top

Getting Started - Deduplication to Tape (Silo Storage)

Getting Started | Advanced

Silo Storage enables you to store deduplicated backups on secondary storage devices. The ability to store deduplicated data on secondary storage reduces the storage requirements and facilitates longer retention periods. The efficient use of storage space enables storing large volumes of backup data, which reduces the cost of backup storage and long term data retention.

Silo Storage also enables effective use of the primary disk storage by managing the disk space and periodically moving the data to the Silo Storage. This efficient disk management reduces the cost of storage.

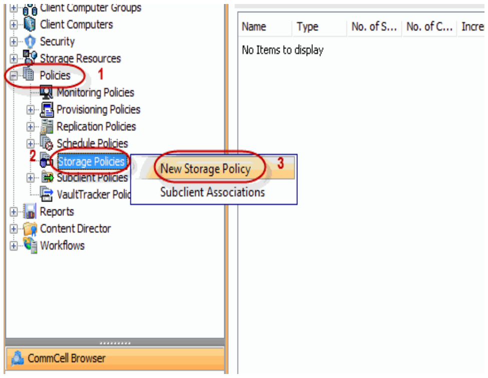
PREREQUISITES

Ensure the following before you setup Silo Storage:

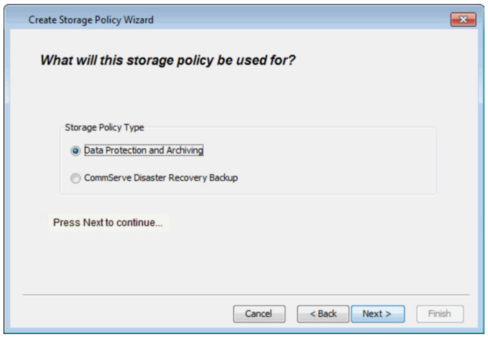
- CommServe and MediaAgent software should be installed.
- Windows File System *i*DataAgent should be installed on CommServe.
- Disk and Tape Libraries are configured.

SET UP SILO STORAGE

1.
- From the CommCell Browser, navigate to and expand **Policies**.
- Right-click **Storage Policies**, and then click **New Storage Policy**.



2. Click **Next**.


Create Storage Policy Wizard

What will this storage policy be used for?

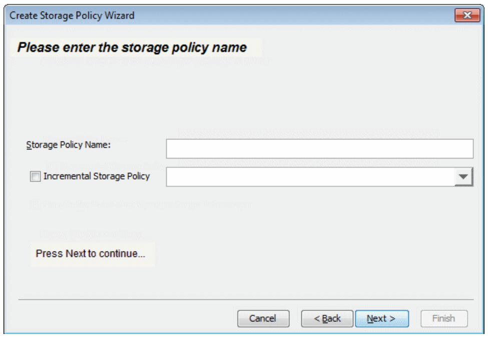
Storage Policy Type

● Data Protection and Archiving

○ CommServe Disaster Recovery Backup

Press Next to continue...

3. Enter the name in the **Storage Policy Name** box and click **Next**.


Create Storage Policy Wizard

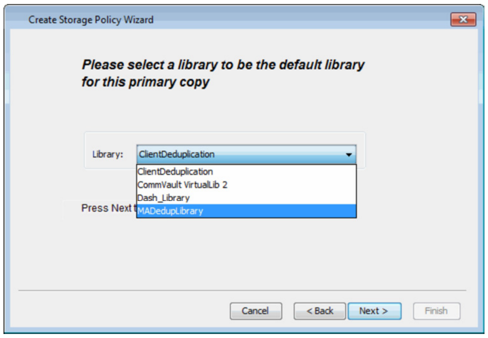
Please enter the storage policy name

Storage Policy Name:

□ Incremental Storage Policy

Press Next to continue...

4. From the **Library** list, click the name of a disk library and click **Next**.


Create Storage Policy Wizard

Please select a library to be the default library for this primary copy

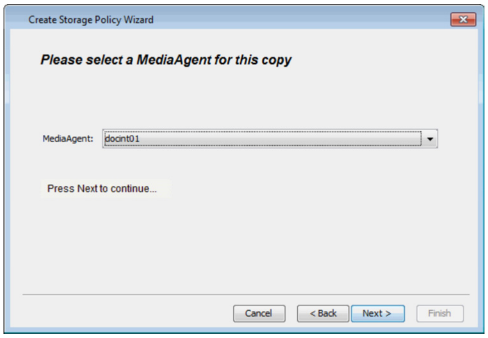
Library: ClientDeduplication

ClientDeduplication
CommVault VirtualLib 2
Dash_Library
MADedupLibrary

Press Next

5. From the **MediaAgent** list, click the name of a MediaAgent that will be used to create the primary copy.

Click **Next**.


Create Storage Policy Wizard

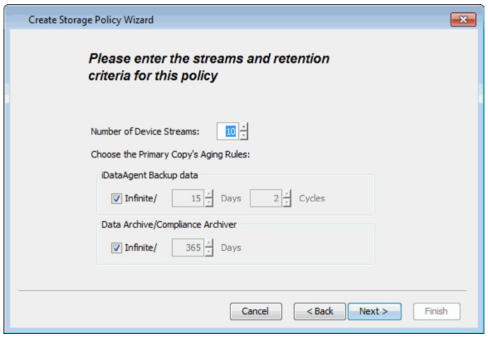
Please select a MediaAgent for this copy

MediaAgent: docint01

Press Next to continue...

6. Click **Next** to accept default values.

If necessary these values can be modified later.


Create Storage Policy Wizard

Please enter the streams and retention criteria for this policy

Number of Device Streams: 10

Choose the Primary Copy's Aging Rules:

iDataAgent Backup data

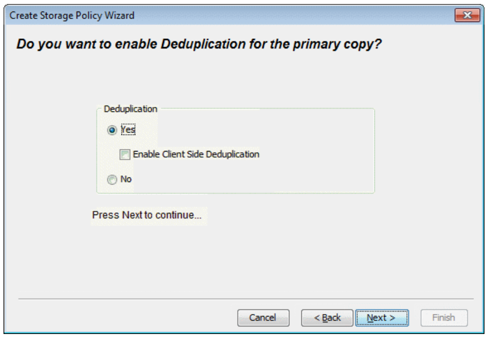
☑ Infinite/ 15 Days 2 Cycles

Data Archive/Compliance Archiver

☑ Infinite/ 365 Days

7.

- Under **Deduplication**, select **Yes**.
- Clear **Enable Client Side Deduplication** check box and click **Next**.


Create Storage Policy Wizard

Do you want to enable Deduplication for the primary copy?

Deduplication

● Yes

☐ Enable Client Side Deduplication

○ No

Press Next to continue...

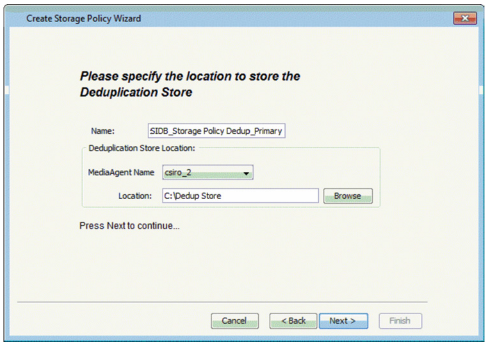
8.

- From the **MediaAgent** list, click the name of the MediaAgent that will be used to store the Deduplication store.

  It can be any MediaAgent which has enough space to store the deduplication store.

- Type the name of the folder in which the deduplication database must be located in the **Deduplication Store Location** or click the **Browse** button to select the folder.
- Click **Next**.

  The deduplication database must be located in a folder and not directly under the root of a disk volume.


Create Storage Policy Wizard

Please specify the location to store the Deduplication Store

Name: SIDB_Storage Policy Dedup_Primary

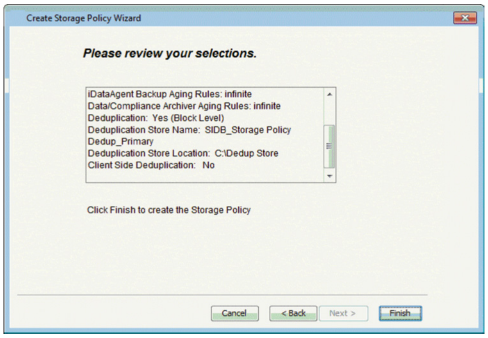
Deduplication Store Location:

MediaAgent Name csiro_2

Location: C:\Dedup Store

Press Next to continue...

9. Click **Finish**.



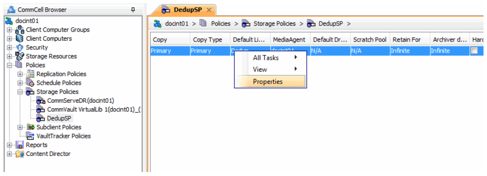
Create Storage Policy Wizard

Please review your selections.

iDataAgent Backup Aging Rules: infinite
Data/Compliance Archiver Aging Rules: infinite
Deduplication: Yes (Block Level)
Deduplication Store Name: SIDB_Storage Policy Dedup_Primary
Deduplication Store Location: C:\Dedup Store
Client Side Deduplication: No

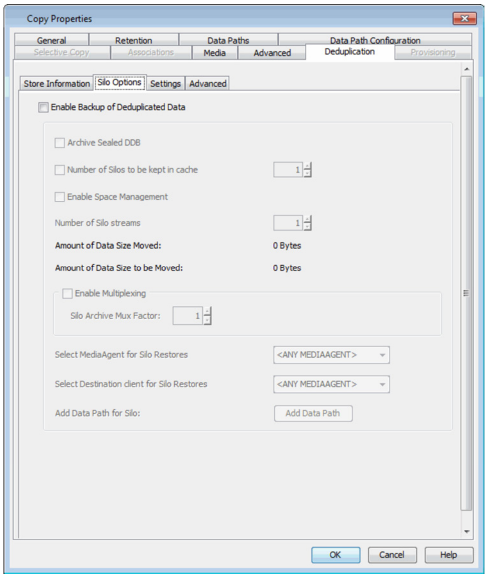
Click Finish to create the Storage Policy

10. - From the CommCell Browser, navigate to **Policies** | **Storage Policies** | ***<Storage_Policy>***.
    - Right-click the primary storage policy copy displayed in the right pane and click **Properties**.



Copy	Copy Type	Default Li...	MediaAgent	Default Dr...	Scratch Pool	Retain For	Archiver d...	Harc
Primary	Primary	Dedup	docint01	N/A	N/A	Infinite	Infinite	□

11. Click the **Deduplication** tab and then click **Silo Option** tab.



□ Enable Backup of Deduplicated Data

□ Archive Sealed DDB

□ Number of Silos to be kept in cache: 1

□ Enable Space Management

Number of Silo streams: 1

Amount of Data Size Moved: 0 Bytes

Amount of Data Size to be Moved: 0 Bytes

□ Enable Multiplexing

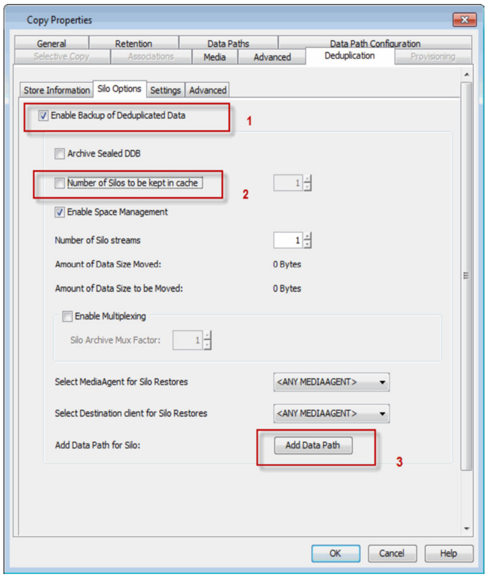
Silo Archive Mux Factor: 1

Select MediaAgent for Silo Restores: <ANY MEDIAAGENT>

Select Destination client for Silo Restores: <ANY MEDIAAGENT>

Add Data Path for Silo: Add Data Path

12. - Select the **Enable Backup of Deduplicated Data** check box.
    - Clear **Number of Silos to be kept in cache** check box.
    - Click **Add Data Path** button.



☑ Enable Backup of Deduplicated Data

□ Archive Sealed DDB

□ Number of Silos to be kept in cache: 1

☑ Enable Space Management

Number of Silo streams: 1

Amount of Data Size Moved: 0 Bytes

Amount of Data Size to be Moved: 0 Bytes

□ Enable Multiplexing

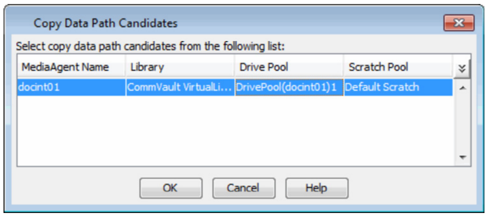
Silo Archive Mux Factor: 1

Select MediaAgent for Silo Restores: <ANY MEDIAAGENT>

Select Destination client for Silo Restores: <ANY MEDIAAGENT>

Add Data Path for Silo: Add Data Path

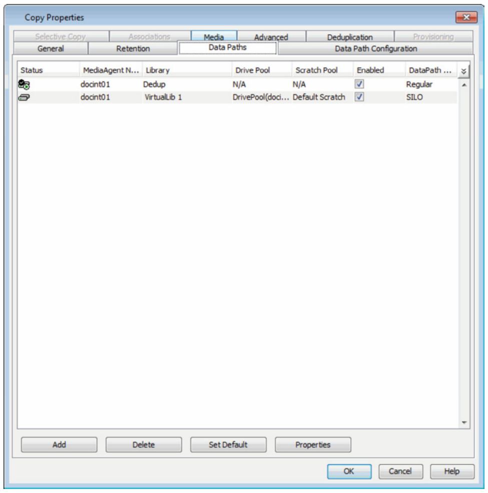
13. Click the **Tape Library** and click **OK**.


Copy Data Path Candidates
Select copy data path candidates from the following list:
OK
Cancel
Help

MediaAgent Name	Library	Drive Pool	Scratch Pool
docint01	CommVault VirtualLi...	DrivePool(docint01)1	Default Scratch

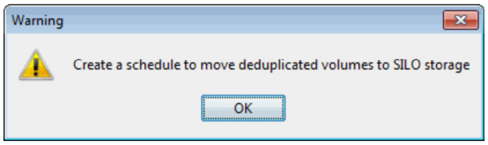
14. The list of data paths will be displayed.

Click **OK**.



Status	MediaAgent N...	Library	Drive Pool	Scratch Pool	Enabled	DataPath ...
	docint01	Dedup	N/A	N/A	☑	Regular
	docint01	VirtualLib 1	DrivePool(doci...	Default Scratch	☑	SILO

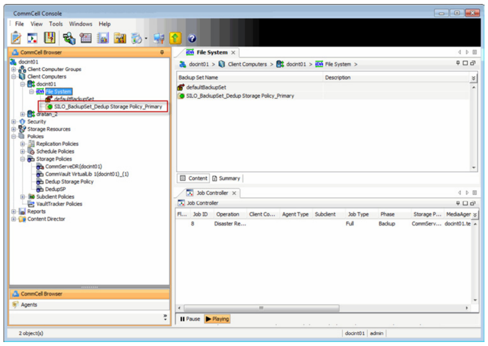
15. Click **OK** to enable the Silo Storage.



Create a schedule to move deduplicated volumes to SILO storage

16.
- From the CommCell Browser, navigate to **Client Computers | *<CommServe_Client>* | File System**.
- A Silo Storage Set with **SILO_BackupSet_*<Storage Policy name>*_*<Storage Policy Copy name>*** naming convention is displayed.

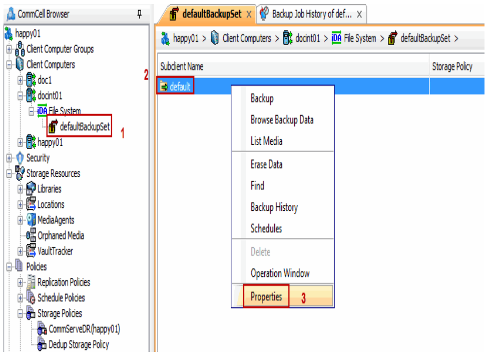
A Silo Storage Set is a special type of On Demand Backup Set containing Silo Storage data. This set must not be modified for any type of operation.



Backup Set Name	Description
defaultBackupSet	
SILO_BackupSet_Dedup Storage Policy_Primary	

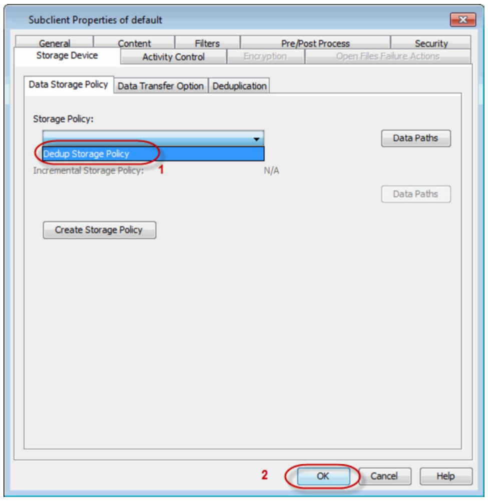
Fl...	Job ID	Operation	Client Co...	Agent Type	Subclient	Job Type	Phase	Storage P...	MediaAger
	8	Disaster Re...				Full	Backup	CommServ...	docint01.te

17.
- From the CommCell Browser, navigate to **Client Computers** | ***<Client>*** | **File System** | **defaultBackupSet**.
- Right-click the subclient in the right pane and click **Properties**.

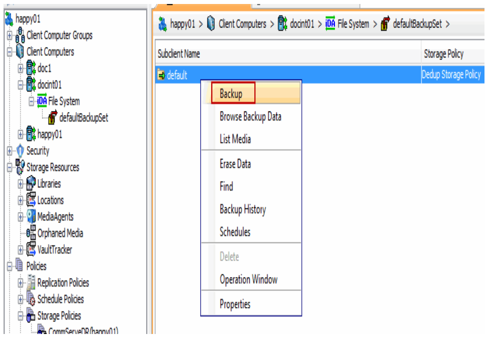


18.
- Click the **Storage Device** tab.
- In the **Storage Policy** list, click the storage policy where the Silo Storage was enabled.
- Click **OK**.

Repeat steps 16-18, in all the subclients that you wish to include this Silo.

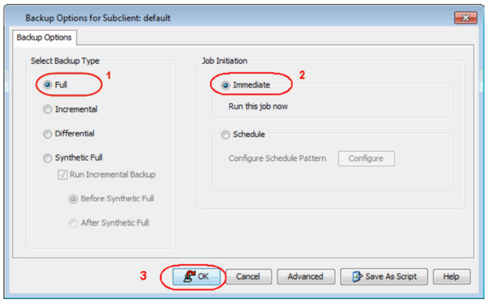


19. - From the CommCell Browser, navigate to **Client Computers | *<Client>* | File System | defaultBackupSet**.
- Right-click the subclient in the right pane and click **Backup**.

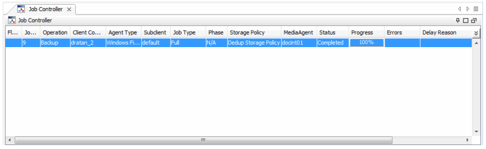


20. - Under **Select Backup Type**, click **Full**.
- Under **Job Initiation**, click **Immediate**.
- Click **OK**.

Repeat steps 19-20, to perform a backup of all subclients included in the Silo.

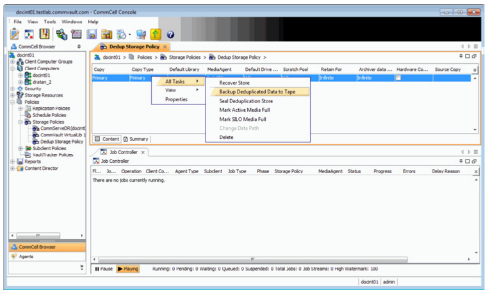


21. You can track the progress of the backup job from the **Job Controller** window. Ensure that the job completes successfully.



Fl...	Jo...	Operation	Client Co...	Agent Type	Subclient	Job Type	Phase	Storage Policy	MediaAgent	Status	Progress	Errors	Delay Reason
	9	Backup	dratan_2	Windows Fi...	default	Full	N/A	Dedup Storage Policy	docint01	Completed	100%		

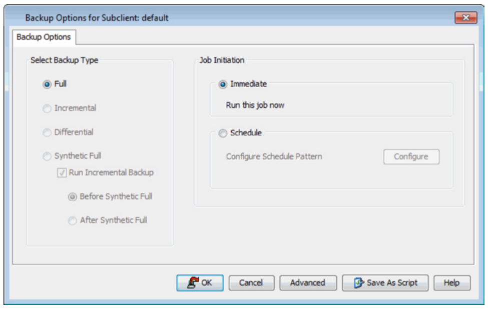
22. - From the CommCell Browser, navigate to **Policies** | **Storage Policies** | ***<Storage_Policy>***.
- Right-click the primary storage policy copy, point to **All Tasks** and then click **Backup Deduplicated Data to Tape**.



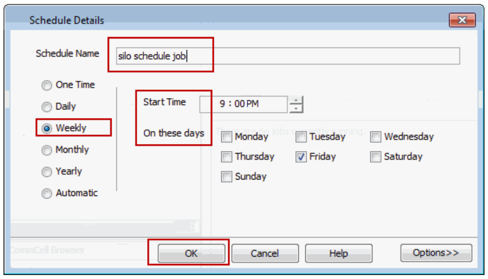
There are no jobs currently running.

Running: 0 Pending: 0 Waiting: 0 Queued: 0 Suspended: 0 Total Jobs: 0 Job Streams: 0 High Watermark: 100

23. - Click **Schedule** to schedule the backup for a specific time.
- Click **Configure** button to set the schedule for the backup job.



24.
- In the **Schedule Name** box, type the name for schedule job.
- Select the appropriate scheduling options. For example:
  - Click **Weekly**.
  - In the **Start Time** box, type or select the time you want to change.
  - Check the days you want the run the job.
- Click **OK**.

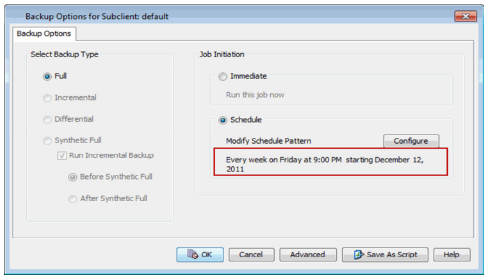

Schedule Name: silo schedule job

Start Time: 9 : 00 PM

On these days: ☐ Monday ☐ Tuesday ☐ Wednesday ☐ Thursday ☑ Friday ☐ Saturday ☐ Sunday

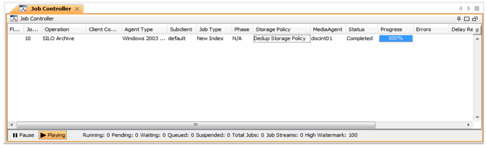
25. Click **OK.**

The Silo backup job will execute as per the schedule.


Modify Schedule Pattern

Every week on Friday at 9:00 PM starting December 12, 2011

26. When the schedule is run, the **Job Controller** window in the CommCell Console will display the job as shown in the sample image.


Fl...	Jo...	Operation	Client Co...	Agent Type	Subclient	Job Type	Phase	Storage Policy	MediaAgent	Status	Progress	Errors	Delay Re
	10	SILO Archive		Windows 2003 ...	default	New Index	N/A	Dedup Storage Policy	docint01	Completed	100%		

Running: 0 Pending: 0 Waiting: 0 Queued: 0 Suspended: 0 Total Jobs: 0 Job Streams: 0 High Watermark: 100

Advanced - Deduplication to Tape (Silo Storage)

Getting Started | Advanced

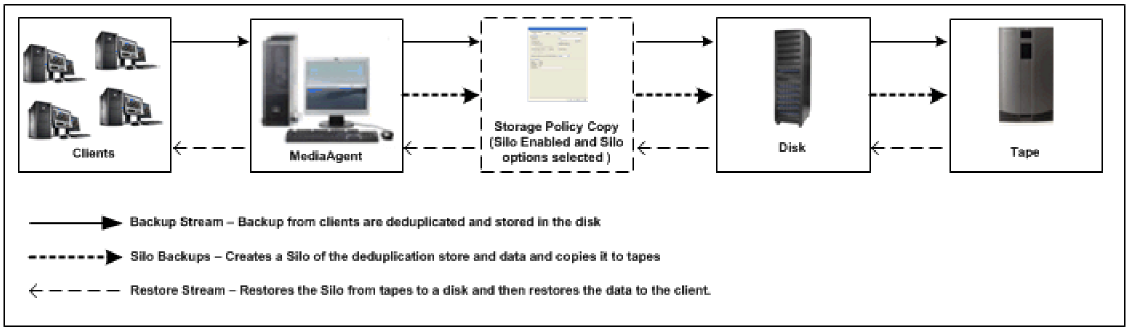
TABLE OF CONTENTS

How Does Silo Work

Silo Storage provides the ability to store deduplicated data in tapes. This is performed as follows:

- Backup data from clients is first deduplicated in a primary disk.
- The deduplicated data, which includes the deduplication store and the data (called as Silos), are then copied to tape by running a Silo backup job.
- During a restore operation, if the data is available in disk it is restored from the disk. If the data is not available, then the necessary tapes are accessed to bring back the data to the disk, and then restored to the client.

The following illustration provides an overview of Silo Storage.


Clients
MediaAgent
Storage Policy Copy (Silo Enabled and Silo options selected)
Disk
Tape
Backup Stream – Backup from clients are deduplicated and stored in the disk
Silo Backups – Creates a Silo of the deduplication store and data and copies it to tapes
Restore Stream – Restores the Silo from tapes to a disk and then restores the data to the client.

To enable Silo Storage in your environment you need to:

- Create a Silo enabled Storage Policy copy
- Use this storage policy to perform backups from your clients by pointing the subclients to the Silo enabled storage policy copy
- Run or schedule silo job to move the data to Silo storage

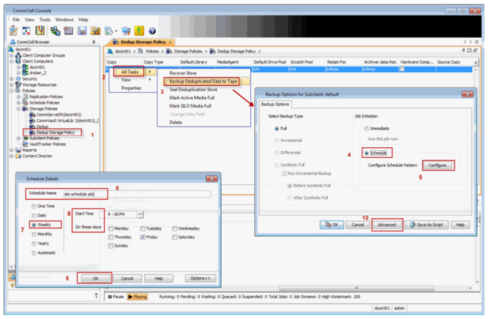
This is explained in the Getting Started section. The following sections describe additional options for managing Silo storage.

Scheduling a Silo Backup

Silo backups copy the deduplication store and the corresponding deduplicated data residing in the disk to tape.

Data from the disk can be moved to tapes on a regular basis by scheduling the silo backup job.

Larger Silos provide better space savings, and smaller silos enables faster restore operations and better Silo manageability.



Schedule Name: silo schedule job
Start Time: 9 : 00 PM

1. From the CommCell Browser, navigate to **Policies** | **Storage Policies** | ***<Storage_Policy>***.
2. Right-click the primary storage policy copy displayed in the right pane, point to **All Tasks** and then click **Backup Deduplicated Data to Tape**.
3. In the **Backup Options for Subclient** dialog box, perform the following:
   - Click **Schedule** to schedule the backup for a specific time.
   - Click **Configure** button to set the schedule for the backup job.
4. In the **Schedule Details** dialog box, perform the following:
   - In the **Schedule Name** box, type the name for schedule job.
   - Select the appropriate scheduling options. For example:

     Click **Weekly**.

In the **Start** box, type or select the time you want to change.

Check the days you want the run the backup job.

5. Click **OK** to close the **Schedule Details** dialog box.
6. Click **OK** to close the **Backup Options for Subclient** dialog box.

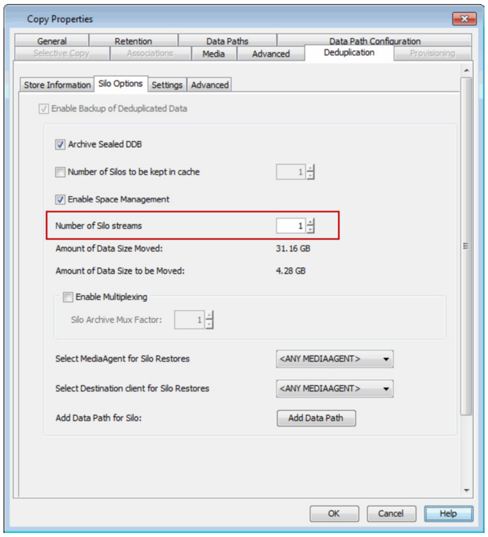
The Silo backup job will execute as per the schedule.

CONFIGURING DATA STREAMS FOR A SILO BACKUP

Silo backup operations are performed using dedicated data streams to avoid the job going into a pending state. These dedicated silo streams are in addition to the data streams configured for the copy.

By default, the system assigns one silo stream per copy. You can add or modify the number of silo streams for each copy.

1. From the CommCell Browser, navigate to **Policies** | **Storage Policies |** ***<Storage_Policy>***.
2. Right-click the primary storage policy copy displayed in the right pane and click **Properties**.
3. Click the **Deduplication** tab, and then click the **Silo Options** tab.
4. In the **Number of Silo streams** box, type or select the number of dedicated data streams you want to change.
5. Click **OK**.



Copy Properties

General | Retention | Data Paths | Data Path Configuration
Selective Copy | Associations | Media | Advanced | Deduplication | Provisioning

Store Information | Silo Options | Settings | Advanced

☑ Enable Backup of Deduplicated Data

☑ Archive Sealed DDB

☐ Number of Silos to be kept in cache: 1

☑ Enable Space Management

Number of Silo streams: 1

Amount of Data Size Moved: 31.16 GB

Amount of Data Size to be Moved: 4.28 GB

☐ Enable Multiplexing

Silo Archive Mux Factor: 1

Select MediaAgent for Silo Restores: <ANY MEDIAAGENT>

Select Destination client for Silo Restores: <ANY MEDIAAGENT>

Add Data Path for Silo:

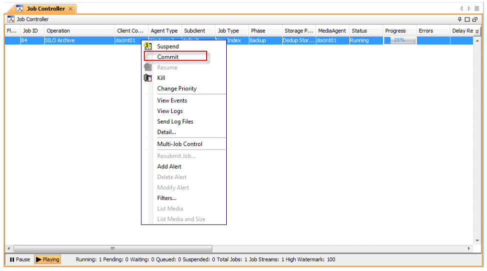
MANAGING SILO BACKUPS

Silo backup jobs can be interrupted and stopped when the job is in progress. This is done by using the **Commit** option in the Job Controller. When used it terminates the silo backup job, by committing the data in the Silo storage as available at that point in time.

The next Silo backup job will automatically start the backup from where the previous backup ended. For example, if the job had to transfer 10 volumes to Silo Storage and you chose the Commit operation while transferring volume 6, the first 5 volumes transferred to Silo storage is committed and the job is successfully completed. The next backup job to Silo Storage will start from volume 6.

1. From the CommCell Browser, in the **Job Controller** window, right-click the silo backup job and click **Commit**.
2. The job status may change to **Interrupt Pending** for a few moments while the operation completes.

   Once operation completed, the job status will change to **Complete**.



Job Controller

Fl...	Job ID	Operation	Client Co...	Agent Type	Subclient	Job Type	Phase	Storage P...	MediaAgent	Status	Progress	Errors	Delay Re
	84	SILO Archive	docint01			Index	Backup	Dedup Stor...	docint01	Running	25%		

Running: 1 Pending: 0 Waiting: 0 Queued: 0 Suspended: 0 Total Jobs: 1 Job Streams: 1 High Watermark: 100

RESTORING FROM A SILO

When a Silo backup is restored, it follows one of the following two sequences:

- If the data is available in the primary disk, it is restored from the primary disk.
- If the data is not available in the primary disk, then the following two phase restore is performed:
  - First the original restore operation goes to Pending state in the Job Controller, and automatically kicks off another job called the Silo Retrieval job to retrieve data from tape to the primary disk.
  - Once the data is available in the primary disk, the original restore operation automatically resumes to restore the data to the restore location.

This two-phase restore is an entirely seamless operation and does not require user intervention. The Job Controller displays both the original restore as well as the Silo Retrieval jobs.

The following sections describe how to restore from a silo.

LIST MEDIA REQUIRED FOR SILO RESTORES

When you perform a restore operation, you must determine whether the data is available in the disk or in the tape. If the data is available in the tape, you must recall the media and have it available in the storage device to successfully complete the restore.

The following steps provides information on how to identify the media:

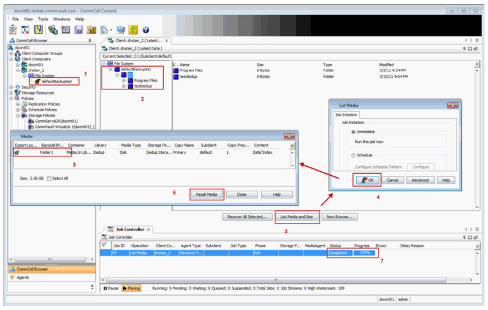
1. From the CommCell Browser, navigate to **Client Computers** | ***<Client>*** | **File System** | **defaultBackupSet**.
2. Right-click the subclient in the right pane and click **Browse Backup Data**.
3. Click **OK**.
4. From the browse window, expand the tree and select the files and/or folders that you wish to restore and then click **List Media and Size** button.
5. Click **OK**.

The Media dialog box, displays the location of the selected data. This could be one of the following:

- Primary disk

  If the data is available in the primary disk, you can proceed with the restore.
- List of tapes
  - If the data is available in tapes and if the tapes are available in the storage device (library) you can proceed with the restore.
  - If the data is available in tapes and if the tapes were removed for off-site storage then click the **Recall Media** button.

    Restart the restore operation once the requested media is available in the storage device.



S... Name	Size	Type	Modified
Program Files	0 Bytes	Folder	3/3/11 4:24 PM
testdedup	0 Bytes	Folder	3/15/11 4:04 PM

Export Loc...	Barcode(M...	Container	Library	Media Type	Storage Po...	Copy Name	Subclient	Copy Prec...	Content
	Folder1	Media In Lib...	Dedup	Disk	Dedup Stora...	Primary	default	1	Data Index

Size: 2.56 GB □ Select All

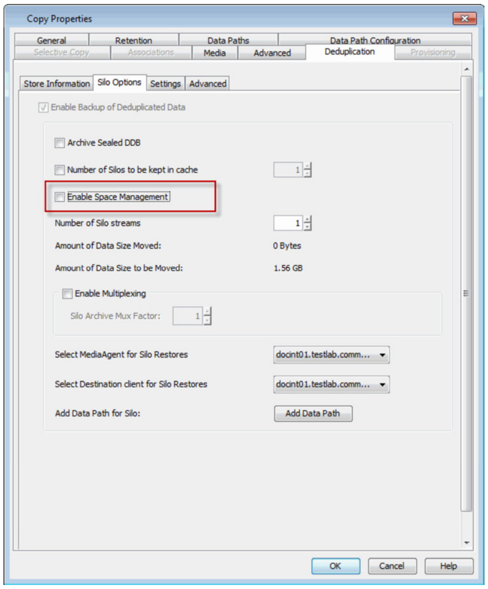
Job ID	Operation	Client Co...	Agent Type	Subclient	Job Type	Phase	Storage P...	MediaAgent	Status	Progress	Errors	Delay Reason
47	List Media	dratan_2	Windows Fi...			N/A			Completed	100%		

Running: 0 Pending: 0 Waiting: 0 Queued: 0 Suspended: 0 Total Jobs: 0 Job Streams: 0 High Watermark: 100

TEMPORARILY DISABLE SPACE MANAGEMENT

Use the following steps to disable space management on the disk. This will ensure sufficient space for silo restores and is useful when restoring large volumes of data from Silo Storage.

1. From the CommCell Browser, navigate to **Policies** | **Storage Policies** | ***<Storage_Policy>***.
2. Right-click the primary storage policy copy displayed in the right pane and click **Properties**.
3. Click the **Deduplication** tab, and then click the **Silo Options** tab.
4. Clear the **Enable Backup of Deduplicated Data** check box.
5. Click **OK**.



☑ Enable Backup of Deduplicated Data

□ Archive Sealed DDB

□ Number of Silos to be kept in cache: 1

□ Enable Space Management

Number of Silo streams: 1

Amount of Data Size Moved: 0 Bytes

Amount of Data Size to be Moved: 1.56 GB

□ Enable Multiplexing

Silo Archive Mux Factor: 1

Select MediaAgent for Silo Restores: docint01.testlab.comm...

Select Destination client for Silo Restores: docint01.testlab.comm...

Add Data Path for Silo:

RESERVE A MOUNT PATH FOR SILO RESTORES

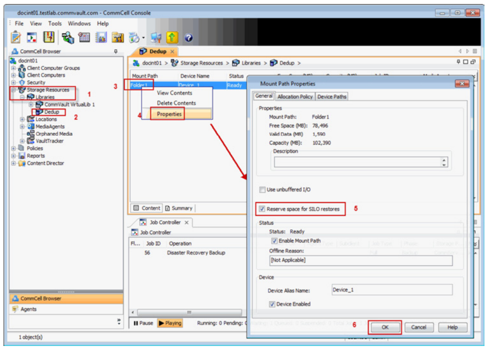
When data from Silo Storage is restored, the Silos are retrieved to the primary media. By default, the Silos are retrieved to the original mount path from which the data was migrated to silo storage. However, during a restore, if the original mount path does not have enough space, the Silos are automatically copied to any other mount path with sufficient space available in the library.

To ensure that a mount path with sufficient space is available in the library at all times, you can have a dedicated mount path that is reserved for Silo restore operations only. When reserved for Silo restores, the number of data writers to the mount path is set to zero and this prevents the mount path from being used for regular backup operations.

When a reserved mount path is available, then all Silo restore operations on the library are run to the mount path by default. It is recommended that the storage capacity on this mount path is equivalent to the size of an average Silo.

The following steps provides information on how to reserve a mount path for Silo restores:

1. From the CommCell Browser, navigate to **Storage Resources | Libraries | *<library>*.**
2. Right-click the mount path in the right pane and then click **Properties**.
3. Select the **Reserve Space for SILO Restores** check box.
4. Click **OK**.



Mount Path: Folder1
Free Space (MB): 78,496
Valid Data (MB): 1,590
Capacity (MB): 102,390

☐ Use unbuffered I/O

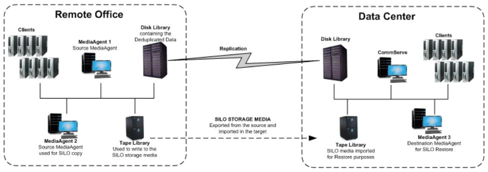
☑ Reserve space for SILO restores

Status: Ready
☑ Enable Mount Path
Offline Reason: [Not Applicable]

Device Alias Name: Device_1
☑ Device Enabled

SELECT A SPECIFIC MEDIAAGENT FOR SILO RESTORES

By default, the Silo restore will be performed on the source MediaAgent which was used to make the Silo backup. If necessary, you can also select a specific MediaAgent to perform the Silo restore. This may be needed in some situations as shown in the diagram.



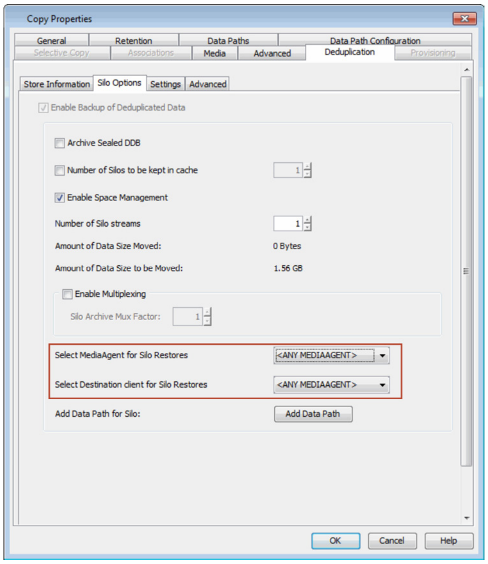
- MediaAgent 1 in a remote office is used to perform deduplicated backup to disk library which is replicated continuously to a disk library in the Data Center.
- MediaAgent 2 is used to perform a Silo copy of the data.
- The resulting media containing the Silo data is moved to the Data Center for storage.

If you need to restore the data from the Silo volume, you can use MediaAgent 3. If you do not use this option, the restore will start in the source which is MediaAgent 2.

In the following procedure you can designate MediaAgent 2 as the Source MediaAgent and MediaAgent 3 as the destination MediaAgent.

1. From the CommCell Browser, navigate to **Policies** | **Storage Policies |** ***<Storage_Policy>***.
2. Right-click the primary storage policy copy displayed in the right pane and click **Properties**.
3. Click the **Deduplication** tab, and then click the **Silo Options** tab.
4. Select source MediaAgent from the **Select MediaAgent for Silo Restores** list.

   As this MediaAgent will be used to access the tape library containing the Silo storage media, ensure to select a MediaAgent that has access to the appropriate storage media containing the Silo enabled source copy.
5. Select destination MediaAgent from the **Select Destination client for Silo Restores** list, to which the Silo volumes must be restored.
6. Click **OK**.



☑ Enable Backup of Deduplicated Data

☐ Archive Sealed DDB

☐ Number of Silos to be kept in cache: 1

☑ Enable Space Management

Number of Silo streams: 1

Amount of Data Size Moved: 0 Bytes

Amount of Data Size to be Moved: 1.56 GB

☐ Enable Multiplexing

Silo Archive Mux Factor: 1

Select MediaAgent for Silo Restores: <ANY MEDIAAGENT>

Select Destination client for Silo Restores: <ANY MEDIAAGENT>

Add Data Path for Silo:

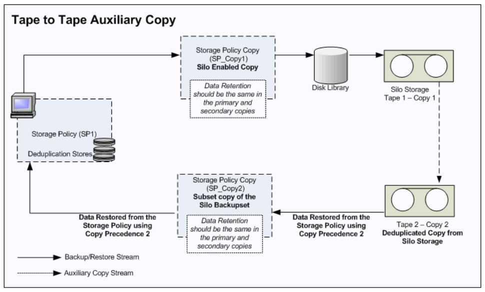
PERFORMING AUXILIARY COPIES WITH SILO STORAGE

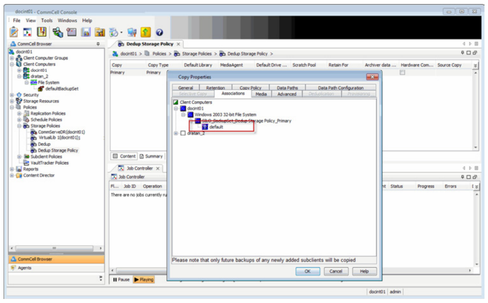
SETUP TAPE-TO-TAPE AUXILIARY COPY

You can perform an Auxiliary Copy of the Silo storage. This Auxiliary Copy will preserve the data deduplication in the Silo Storage and can be used to make the additional copies of the data.

The diagram illustrates the tape-to-tape Auxiliary Copy with Silo Storage.

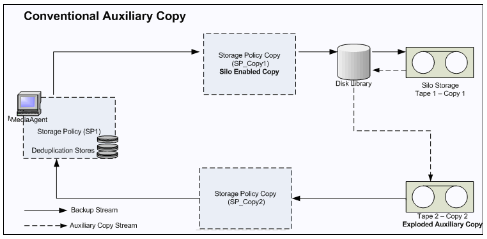
Use the following steps to setup tape-to-tape auxiliary copy:


Tape to Tape Auxiliary Copy
Storage Policy Copy
(SP_Copy1)
Silo Enabled Copy
Data Retention should be the same in the primary and secondary copies
Disk Library
Silo Storage
Tape 1 – Copy 1
Storage Policy (SP1)
Deduplication Stores
Storage Policy Copy
(SP_Copy2)
Subset copy of the Silo Backupset
Data Retention should be the same in the primary and secondary copies
Data Restored from the Storage Policy using Copy Precedence 2
Data Restored from the Storage Policy using Copy Precedence 2
Tape 2 – Copy 2
Deduplicated Copy from Silo Storage
Backup/Restore Stream
Auxiliary Copy Stream



1. From the CommCell Browser, navigate to **Policies** | **Storage Policies.**
2. Right-click the primary storage policy containing the silo enabled storage policy copy, and then click **Properties**.
3. Click **Retention** tab, and note down the values specified in the **Basic Retention Rule for All Backups** area.
4. Click **OK**.
5. From the CommCell Browser, navigate to **Policies | Storage Policies | <Storage_Policy>**.
6. Right-click **<storage_policy>**, point to **All Tasks** and then click **Create New Copy**.
7. Specify name in **Copy Name**.
8. From the **Library** list, click the name of a tape library.
9. From the **MediaAgent** list, click the name of a MediaAgent.
10. From the **Drive Pool** list, click the name of the drive pool.
11. From the **Scratch Poo**l list, click the name of the default scratch.
12. Click **Associations** tab.
13. Clear **Client Computers** and navigate to **Client Computers | *<CommServe_Client>* | Windows File System** | **SILO_BackupSet_*<Storage Policy name>*_*<Storage Policy Copy name>*** and then select **default**.
14. Click the **Retention** tab.
15. Enter the same data retention values in the **Basic Retention Rules for All Backups** area, that you noted in the above steps from primary copy.
16. Click **OK**.
17. Right-click **<storage_policy>**, point to **All Tasks** and then click **Run Auxiliary Copy**.
18. Click **OK**.

CONVENTIONAL AUXILIARY COPY



A conventional Auxiliary Copy stores the original data without preserving the data deduplication. Use the conventional Auxiliary Copy if you wish to retain a copy of the complete data, without the deduplication.

The conventional Auxiliary Copy is done as follows:

- If the data is available in the primary disk, it is unraveled in the primary disk and copied to tape.
- If the data is not available in the primary disk, then the following two phase Auxiliary Copy operation is performed:
  - First the original Auxiliary Copy operation goes to Pending state in the Job Controller, and automatically kicks off another job called the Silo Retrieval job to retrieve data from tape to the primary disk.
  - Once the data is available in the primary disk, it is unraveled in the primary disk and copied to tape.

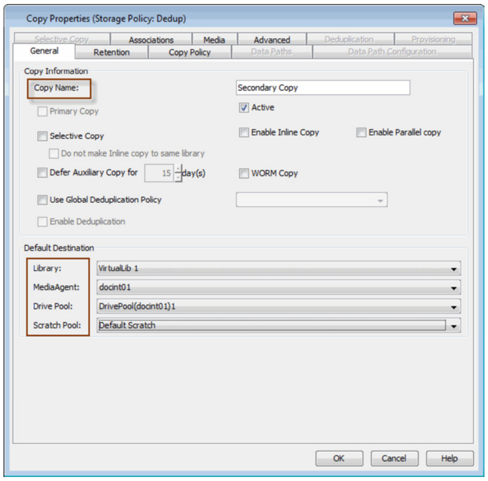
To restore data from such copy, set the copy precedence as described in Restore From A Copy.

Use the following steps to setup a conventional Auxiliary Copy:

1. From the CommCell Browser, navigate to **Policies** | **Storage Policies.**
2. Right-click the primary storage policy containing the silo enabled storage policy copy, and then click **Properties**.
3. Click **Retention** tab, and note down the values specified in the **Basic Retention**

Rule for All Backups area.

4. Click **OK**.
5. From the CommCell Browser, navigate to **Policies | Storage Policies | <Storage_Policy>**.
6. Right-click **<storage_policy>**, point to **All Tasks** and then click **Create New Copy**.
7. Specify name in **Copy Name**.
8. From the **Library** list, click the name of a tape library.
9. From the **MediaAgent** list, click the name of a MediaAgent.
10. From the **Drive Pool** list, click the name of the drive pool.
11. From the **Scratch Poo**l list, click the name of the default scratch.
12. Click the **Retention** tab.
13. Enter the same data retention values in the **Basic Retention Rules for All Backups** area, that you noted in the above steps from primary copy.
14. Click **OK**.
15. Right-click **<storage_policy>**, point to **All Tasks** and then click **Run Auxiliary Copy**.
16. Click **OK**.


Copy Properties (Storage Policy: Dedup)

Copy Information

Copy Name: Secondary Copy

□ Primary Copy ☑ Active

□ Selective Copy □ Enable Inline Copy □ Enable Parallel copy

□ Do not make Inline copy to same library

□ Defer Auxiliary Copy for 15 day(s) □ WORM Copy

□ Use Global Deduplication Policy

□ Enable Deduplication

Default Destination

Library: VirtualLib 1

MediaAgent: docint01

Drive Pool: DrivePool(docint01)1

Scratch Pool: Default Scratch

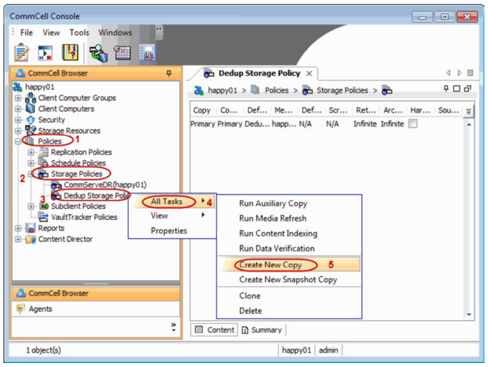
ENABLING SILO IN A SECONDARY COPY

You can have a non-silo primary copy to backup data without deduplication and then enable silo in the secondary copy. The data from the primary copy is deduplicated on a primary disk and the silo's are then moved to a tape when a silo backup is run on the secondary copy.

Use the following steps to create a silo enabled secondary copy:

1.

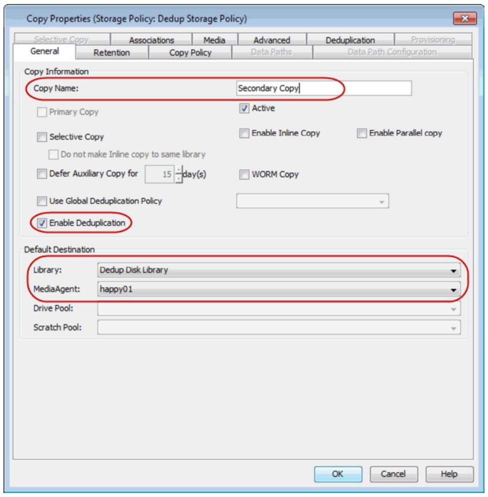
- From the CommCell Browser, navigate to **Policies** | **Storage Policies | *<Storage_Policy>***.
- Right-click ***<storage_policy>***, point to **All Tasks** and then click **Create New Copy**.



2.

- Specify name in **Copy Name**.
- From the **Library** list, click the name of a disk library.
- From the **MediaAgent** list, click the name of a MediaAgent.
- Select **Enable Deduplication** box. The **Deduplication** tab is enabled.
- Click **Deduplication** tab.

Deduplication can only be enabled for storage policy copies associated with a disk library.


Copy Properties (Storage Policy: Dedup Storage Policy)

Copy Information

Copy Name: Secondary Copy

□ Primary Copy ☑ Active

□ Selective Copy □ Enable Inline Copy □ Enable Parallel copy

□ Do not make Inline copy to same library

□ Defer Auxiliary Copy for 15 day(s) □ WORM Copy

□ Use Global Deduplication Policy

☑ Enable Deduplication

Default Destination

Library: Dedup Disk Library

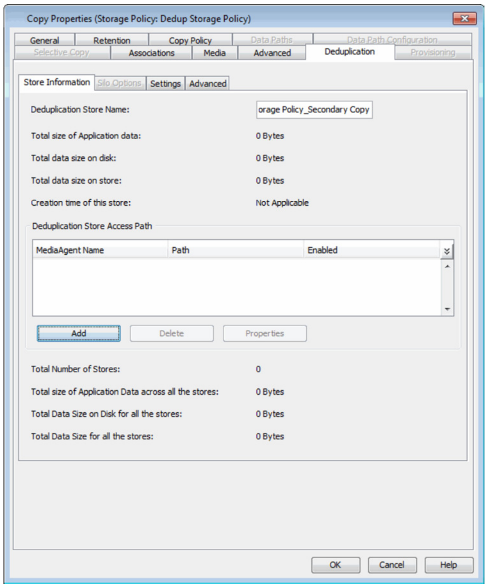
MediaAgent: happy01

Drive Pool:

Scratch Pool:

3.

- The default name of the deduplication store is displayed in **Deduplication Store Name** box.
- In the **Deduplication Store Access Path** area, click **Add.**



Copy Properties (Storage Policy: Dedup Storage Policy)

Deduplication Store Name: orage Policy_Secondary Copy

Total size of Application data: 0 Bytes

Total data size on disk: 0 Bytes

Total data size on store: 0 Bytes

Creation time of this store: Not Applicable

Deduplication Store Access Path

MediaAgent Name	Path	Enabled

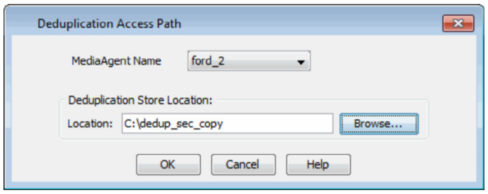
Total Number of Stores: 0

Total size of Application Data across all the stores: 0 Bytes

Total Data Size on Disk for all the stores: 0 Bytes

Total Data Size for all the stores: 0 Bytes

4.
- From the **MediaAgent** list, click the name of a MediaAgent.
- Type the name of the folder in which the deduplication database must be located in the **Deduplication Store Location** or click the **Browse** button to select the folder.
- Click **OK**.



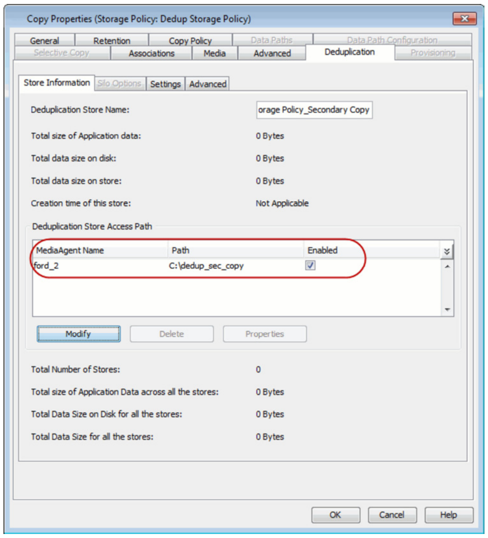
Deduplication Access Path

MediaAgent Name: ford_2

Deduplication Store Location:

Location: C:\dedup_sec_copy

5.
- The store information is displayed in the **Deduplication Store Access Path** area.
- Click **OK**.



Copy Properties (Storage Policy: Dedup Storage Policy)

Deduplication Store Name: orage Policy_Secondary Copy

Total size of Application data: 0 Bytes

Total data size on disk: 0 Bytes

Total data size on store: 0 Bytes

Creation time of this store: Not Applicable

Deduplication Store Access Path

MediaAgent Name	Path	Enabled
ford_2	C:\dedup_sec_copy	☑

Total Number of Stores: 0

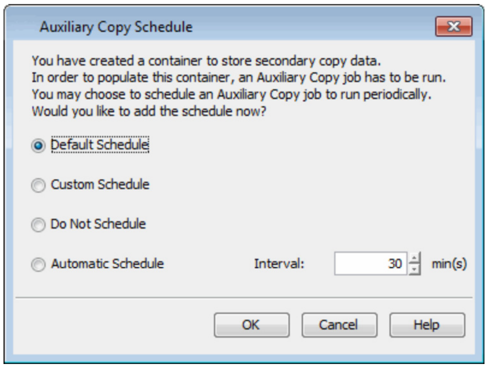
Total size of Application Data across all the stores: 0 Bytes

Total Data Size on Disk for all the stores: 0 Bytes

Total Data Size for all the stores: 0 Bytes

6.

Click **OK** to accept the default schedule.



Auxiliary Copy Schedule

You have created a container to store secondary copy data.
In order to populate this container, an Auxiliary Copy job has to be run.
You may choose to schedule an Auxiliary Copy job to run periodically.
Would you like to add the schedule now?

● Default Schedule

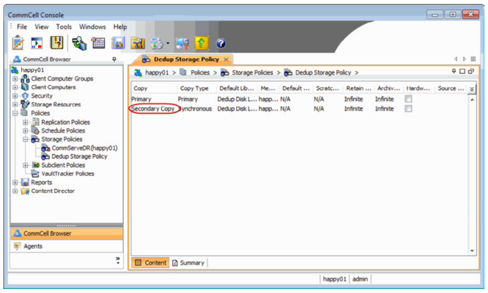
○ Custom Schedule

○ Do Not Schedule

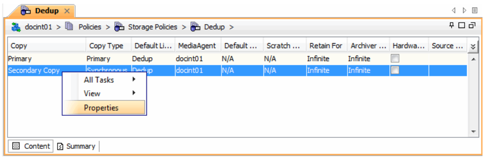
○ Automatic Schedule Interval: 30 min(s)

7.

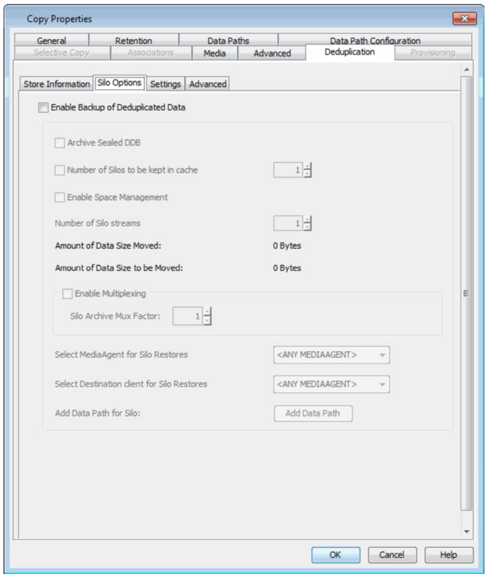
Secondary Copy is displayed in the **Storage Policy** pane.



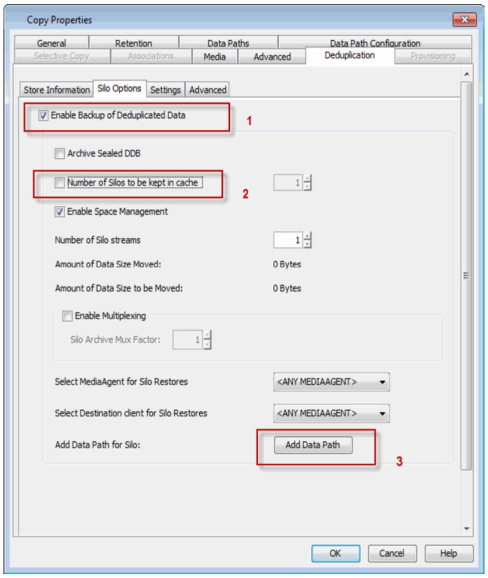
8.
- From the CommCell Browser, navigate to **Policies** | **Storage Policies** | ***<Storage_Policy>***.
- Right-click the Secondary storage policy copy displayed in the right pane and click **Properties**.



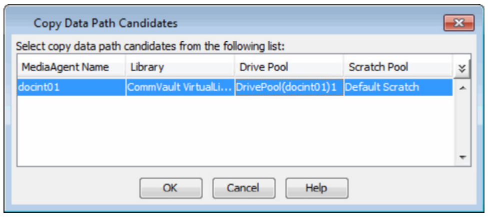
9. Click the **Deduplication** tab and then click **Silo Option** tab.



10.
- Select the **Enable Backup of Deduplicated Data** check box.
- Clear **Number of Silos to be kept in cache** check box.
- Click **Add Data Path** button.



11. Click the **Tape Library** and click **OK**.



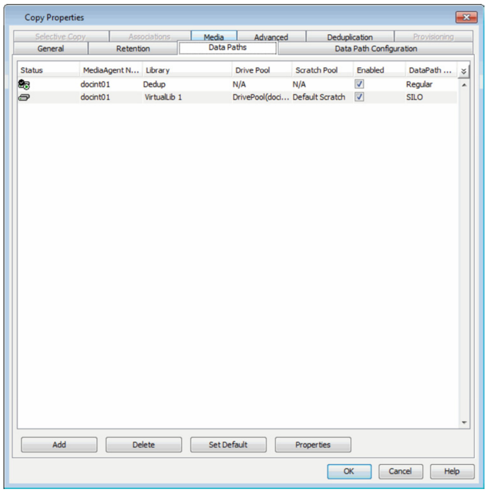
Copy Data Path Candidates

Select copy data path candidates from the following list:

MediaAgent Name	Library	Drive Pool	Scratch Pool
docint01	CommVault VirtualLi...	DrivePool(docint01)1	Default Scratch

12. The list of data paths will be displayed.

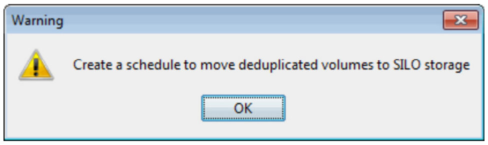
Click **OK**.



Copy Properties

Status	MediaAgent N...	Library	Drive Pool	Scratch Pool	Enabled	DataPath ...
	docint01	Dedup	N/A	N/A	☑	Regular
	docint01	VirtualLib 1	DrivePool(doci...	Default Scratch	☑	SILO

13. Click **OK** to enable the Silo Storage.

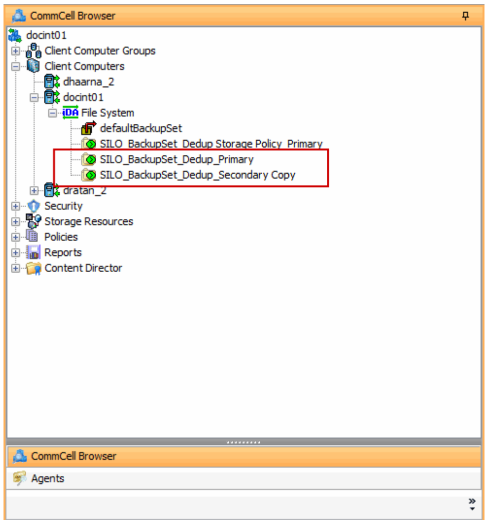


Warning

Create a schedule to move deduplicated volumes to SILO storage

14.
- From the CommCell Browser, navigate to **Client Computers | *<CommServe_Client>* | File System**.
- A Silo Storage Set with **SILO_BackupSet_*<Storage Policy name>*_*<Storage Policy Copy name>*** naming convention is displayed.

A Silo Storage Set is a special type of On Demand Backup Set containing Silo Storage data. This set must not be modified for any type of operation.



RESTORE FROM A COPY

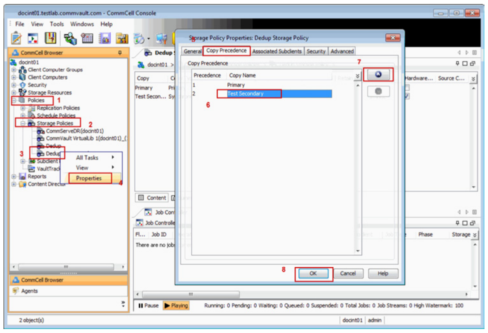
Data can be restored from a tape-to-tape copy. This can be done in one of the following ways:

Use the following steps to restore data from the secondary copy to all clients.

1. From the CommCell Browser, navigate to **Policies** | **Storage Policies.**
2. Right-click **<storage_policy>** and then click **Properties**.
3. Click **Copy Precedence** tab.
4. Select the tape-to-tape auxiliary copy and click the arrow buttons to change its copy precedence to 1.

   The arrows will move to a higher or lower precedence in increments of 1.

5. Click **OK**.

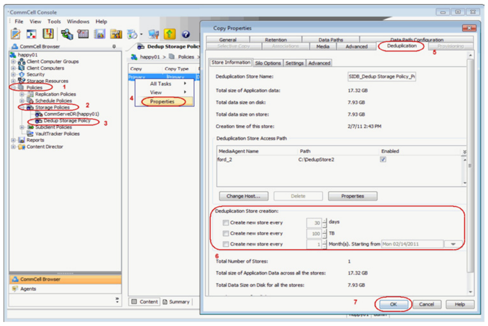


MANAGING DEDUPLICATION STORE

CREATE DEDUPLICATION STORE

By default, a new deduplication store is created for every 100 TB of data. Note that this is the amount of data stored on the media after deduplication. Depending upon your configuration and requirement, deduplication store creation can be configured based on the following parameters:

- Create Store every 'n' number of days.
- Create Store every 'n' TB.



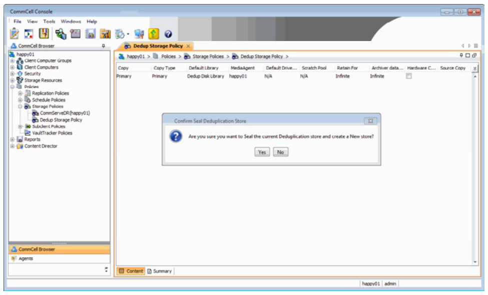
1. From the CommCell Browser, navigate to **Policies** | **Storage Policies | *<Storage_Policy>***.
2. Right-click the primary storage policy copy displayed in the right pane and click **Properties**.
3. Click the **Deduplication** tab.
4. In the **Deduplication Store Creation**, select one of the following:
   - Select **Create new store every - days** and specify the number of days after which a new deduplication store must be created.
   - Select **Create new store every - TB** and specify the size of the store, reaching which a new deduplication store must be created.

     > If above both options are set, a new deduplication store will be created if either one of the two conditions is satisfied.

   - Select **Create new store every - Month(s). Starting from...** and specify the month and start date for a new deduplication store creation.
5. Click **OK**.

SEAL DEDUPLICATION STORE

An active deduplication store can also be sealed on-demand. If the deduplication store contains critical data that must be protected for compliance purposes, or the deduplication store must be moved to Silo Storage immediately to preserve the data, you can seal the currently open deduplication store on-demand and initiate a Silo Backup to move the data to Silo Storage. Once the volume is closed, the data is moved to Silo Storage after 8 hours by default.


Confirm Seal Deduplication Store

Are you sure you want to Seal the current Deduplication store and create a New store?

1. From the CommCell Browser, navigate to **Policies** | **Storage Policies | *<Storage_Policy>***.
2. Right-click the primary storage policy copy displayed in the right pane, point to **All Tasks** and then click **Seal Deduplication Store**.
3. Click **Yes** on the **Confirm Seal Deduplication Store** dialog box.

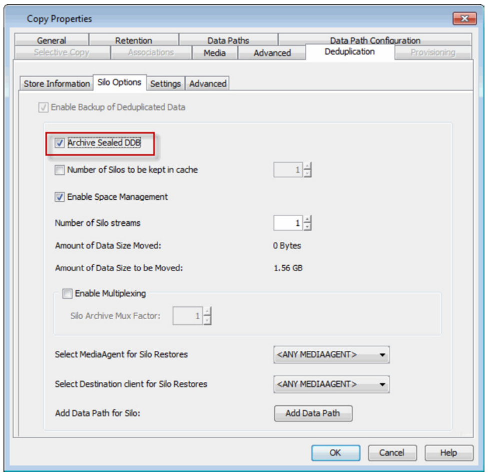
The current active deduplication store will be sealed and the data will be moved automatically to Silo Storage after 8 hours.

ARCHIVE DEDUPLICATION STORE

Silo can be set to automatically archive the deduplication store after you seal it. Archiving the deduplication store frees up disk space by moving the sealed store to Silo Storage.

Deduplication store can be Archived as follows:

1. From the CommCell Browser, navigate to **Policies** | **Storage Policies** | ***<Storage_Policy>***.
2. Right-click the primary storage policy copy displayed in the right pane and click **Properties**.
3. Click the **Deduplication** tab and then click the **Silo Options** tab.
3. Click **Enable Backup of Deduplicated Data**.
4. Click **Archive Sealed DDB.**
5. Click **OK**.



Copy Properties

General | Retention | Data Paths | Data Path Configuration | Selective Copy | Associations | Media | Advanced | Deduplication | Provisioning

Store Information | Silo Options | Settings | Advanced

☑ Enable Backup of Deduplicated Data

☑ Archive Sealed DDB

☐ Number of Silos to be kept in cache: 1

☑ Enable Space Management

Number of Silo streams: 1

Amount of Data Size Moved: 0 Bytes

Amount of Data Size to be Moved: 1.56 GB

☐ Enable Multiplexing

Silo Archive Mux Factor: 1

Select MediaAgent for Silo Restores: <ANY MEDIAAGENT>

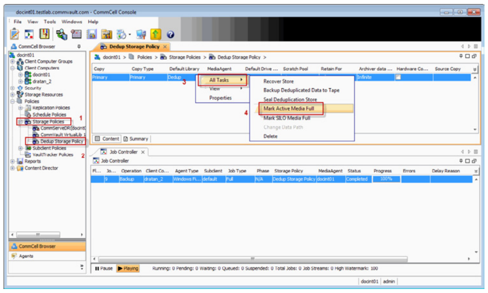
Select Destination client for Silo Restores: <ANY MEDIAAGENT>

Add Data Path for Silo: Add Data Path

MARK THE ACTIVE MEDIA FULL

Use the following steps to mark the active media full before running a Silo backup:

1. From the CommCell Browser, navigate to **Policies** | **Storage Policies** | ***<Storage_Policy>***.
2. Right-click the primary storage policy copy, point to **All Tasks** and then click **Mark Active Media Full**.
3. Click **Yes** on the **Confirm Mark Active Volumes Full** dialog box.
4. Click **OK**.



MANAGING SILOS

SETUP MULTIPLE DATA PATHS TO A SILO

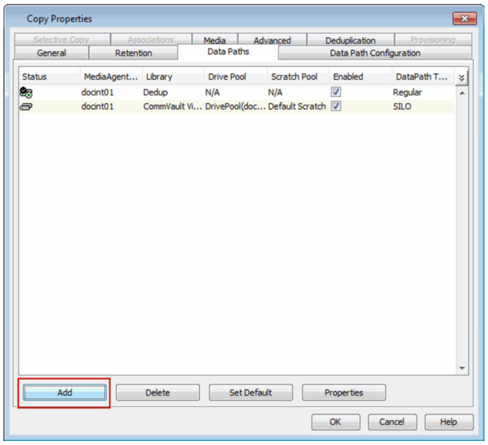
A Storage Policy Copy can be configured to use more than one Silo data path. Use the following steps to setup multiple data paths:

If the data paths are from multiple MediaAgents, then ensure that the index cache is shared between all the MediaAgents associated with the Silo data paths as well as the MediaAgent associated with the primary disk mount path.

All data paths must have read/write permission from all MediaAgents.

1. From the CommCell Browser, navigate to **Policies** | **Storage Policies** | ***<Storage_Policy>***.
2. Right-click the primary storage policy copy displayed in the right pane and click **Properties**.
3. Click the **Data Paths** tab.
4. Click **Add** button to add the multiple data paths.

   When using multiple silo data paths, the data paths are used based on the criteria defined in the **Data Path Configuration** tab.
5. Click **OK**.



Copy Properties

Selective Copy | Associations | Media | Advanced | Deduplication | Provisioning | General | Retention | Data Paths | Data Path Configuration

Status	MediaAgent...	Library	Drive Pool	Scratch Pool	Enabled	DataPath T...
	docint01	Dedup	N/A	N/A	☑	Regular
	docint01	CommVault Vi...	DrivePool(doc...	Default Scratch	☑	SILO

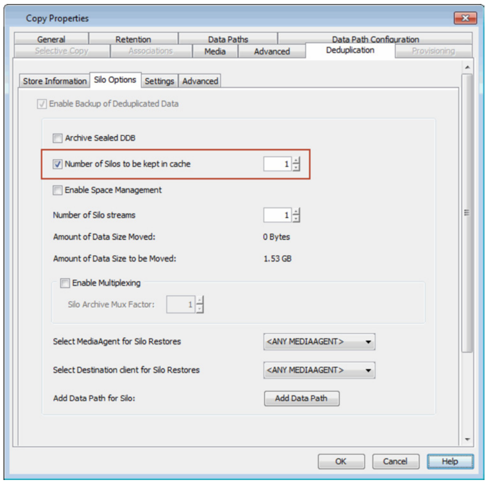
RETAIN SILOS IN THE LOCAL CACHE

The recently moved silo(s) can be retained in the local cache. This eliminates the need to restore the data from the Silo Storage to the primary disk.

Use the following steps to configure the number of silos that must be maintained in the local cache.

> The number of silos to be retained corresponds to the silos that are moved to the silo storage and does not include the ones recalled during restores. For example, if you set the value to 3, the currently active Silo and two recently closed Silos would be retained in the local cache. If you set this value to 0, no silo is retained in the the cache.

1. From the CommCell Browser, navigate to **Policies** | **Storage Policies |** ***<Storage_Policy>***.
2. Right-click the primary storage policy copy displayed in the right pane and click **Properties**.
3. Click the **Deduplication** tab, and then click the **Silo Options** tab.
4. In the **Number of Silos to be kept in cache** box, type or select the number of dedicated data streams you want to change. The default value is set to 1.
5. Click **OK**.



☑ Enable Backup of Deduplicated Data

□ Archive Sealed DDB

☑ Number of Silos to be kept in cache: 1

□ Enable Space Management

Number of Silo streams: 1

Amount of Data Size Moved: 0 Bytes

Amount of Data Size to be Moved: 1.53 GB

□ Enable Multiplexing

Silo Archive Mux Factor: 1

Select MediaAgent for Silo Restores: <ANY MEDIAAGENT>

Select Destination client for Silo Restores: <ANY MEDIAAGENT>

Add Data Path for Silo:

DATA ENCRYPTION ON SILO STORAGE

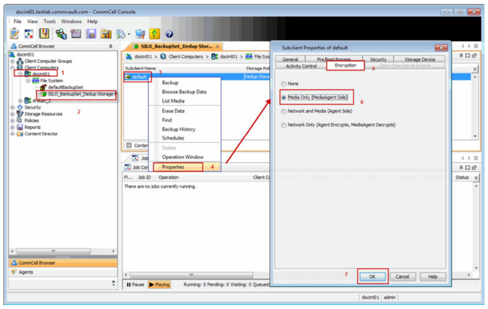
Silo Storage provides data encryption options during data transmission over networks and for storage on media. When data is migrate to offsite storage, data encryption increases the security and integrity of the data.

Use the following steps to enable data encryption:

1. From the CommCell Browser, navigate to **Client Computers**.
2. Right-click the **<CommServe Client>** and then click **Properties**.
3. Click **Encryption** tab, and then click the **Encrypt Data** check box.

   > The **Pass Phrase** is not supported for encryption on Silo Storage.

4. Navigate to **Client Computers |** ***<CommServe_Client>*** **| File System** | **SILO_BackupSet_*<Storage Policy name>_<Storage Policy Copy name>.***
5. Right-click the <subclient> displayed in the right pane and click **Properties**.
6. Click the **Encryption** tab.
7. Click the **Media Only (MediaAgent Side)**.
8. Click **OK**.

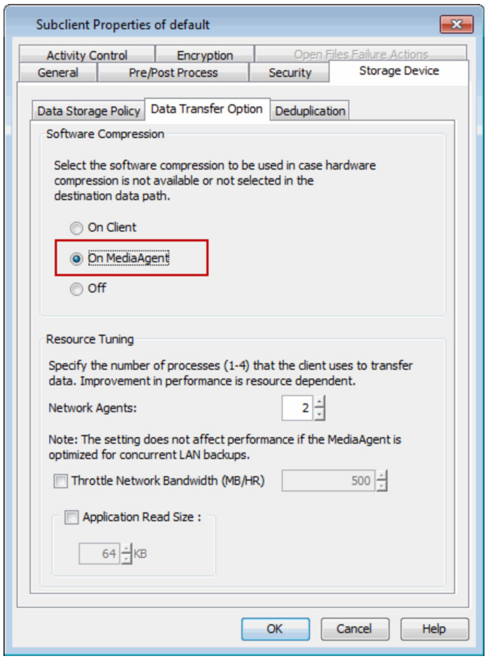


DATA COMPRESSION ON SILO STORAGE

Data migrated to Silo Storage can be stored in compressed format. Compression reduces the quantity of data sent to storage, often doubling the effective capacity of the media (depending on the nature of the data.) This provides the option to have the data in the primary storage in its original form, and enable data compression when the data is migrated to Silo Storage.

> If hardware compression is enabled, then software compression is ignored during Silo backups.

1. From the CommCell Browser, navigate to **Client Computers |** ***<CommServe_Client>*** **| File System** | **SILO_BackupSet_*<Storage Policy name>_<Storage Policy Copy name>.***
2. Right-click the <subclient> displayed in the right pane and click **Properties**.
3. Click the **Storage Device** tab and then click the **Data Transfer Option** tab.
4. In **Software Compression** area, click **On MediaAgent**.
5. Click **OK**.



Software Compression

Select the software compression to be used in case hardware compression is not available or not selected in the destination data path.

○ On Client
● On MediaAgent
○ Off

Resource Tuning

Specify the number of processes (1-4) that the client uses to transfer data. Improvement in performance is resource dependent.

Network Agents: 2

Note: The setting does not affect performance if the MediaAgent is optimized for concurrent LAN backups.

□ Throttle Network Bandwidth (MB/HR) 500

□ Application Read Size :

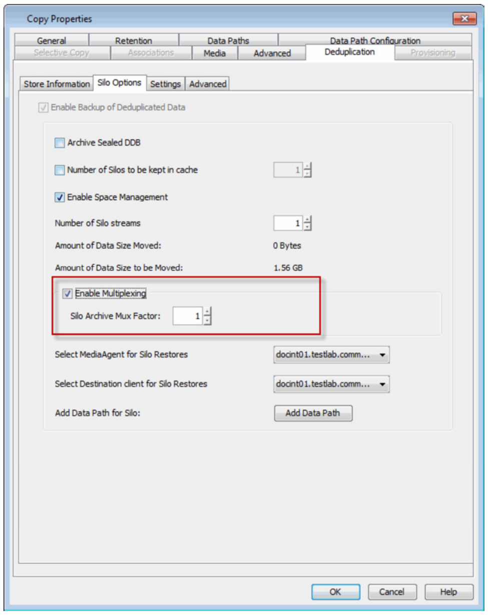
64 KB

DATA MULTIPLEXING FOR SILO OPERATIONS

If the data to be backed up is spread over multiple mount paths having multiple data streams, then you can use the data multiplexing to combine the streams during the write operation. Data multiplexing increases the speed of write operations. This feature is particularly useful in case of high-speed tape drives to fully utilize the high throughput. See Data Multiplexing for a detailed discussion on data multiplexing.

Multiplexing factor is the number of data streams that are backed up concurrently to the same media. See Determining the Multiplexing Factor for more information on how to decide the multiplexing factor.

1. From the CommCell Browser, navigate to **Policies** | **Storage Policies |** ***<Storage_Policy>***.
2. Right-click the primary storage policy copy displayed in the right pane and click **Properties**.
3. Click the **Deduplication** tab, and then click the **Silo Options** tab.
4. Select the **Enable Multiplexing** check box.
5. In the **Silo Archive Mux Factor** box, type or select the number of multiplexing factor for silo operations. The default value is set to 1.
6. Click **OK**.



☑ Enable Backup of Deduplicated Data

□ Archive Sealed DDB

□ Number of Silos to be kept in cache 1

☑ Enable Space Management

Number of Silo streams 1

Amount of Data Size Moved: 0 Bytes

Amount of Data Size to be Moved: 1.56 GB

☑ Enable Multiplexing

Silo Archive Mux Factor: 1

Select MediaAgent for Silo Restores docint01.testlab.comm...

Select Destination client for Silo Restores docint01.testlab.comm...

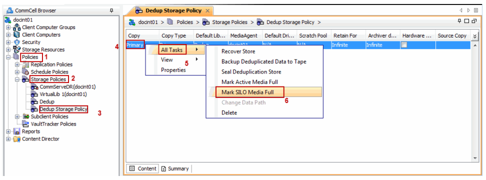
Add Data Path for Silo:

MARK THE SILO MEDIA FULL

Use the following steps to mark the Silo tape as full:

1. From the CommCell Browser, navigate to **Policies** | **Storage Policies |** ***<Storage_Policy>***.
2. Right-click the primary storage policy copy, point to **All Tasks** and then click **Mark SILO Media Full**.

3. Click **Yes** on the **Confirm Mark SILO Volumes Full** dialog box.
4. Click **OK**.



RECLAIMING DISK SPACE AFTER MOVING DATA TO SILO

Silo space management provides disk cleanup options to automatically reclaim the primary disk space once the data is moved to Silo Storage. Disk space occupied by the deduplication store and the associated deduplicated data can be effectively managed and reclaimed as follows:

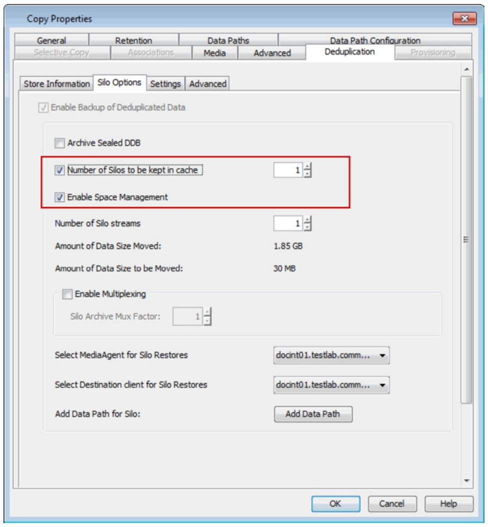
- Only data from the disk media that has been moved to Silo Storage is considered for removal.
- The removal of data is based on a LRU (Least Recently Used) algorithm.

The following exceptions apply:

- If a Silo is retained in the local disk cache (as described in Retain Silos in the Local Cache), it will not be considered for removal.
- If the Storage Policy Copy is configured for Auxiliary Copy, Data Verification, or Offline Content Indexing, then the copy data is not removed until all dependency are fulfilled.

Use the following steps to enable Silo Space Management:

1. From the CommCell Browser, navigate to **Policies** | **Storage Policies | *<Storage_Policy>***.
2. Right-click the primary storage policy copy displayed in the right pane and click **Properties**.
3. Click the **Deduplication** tab, and then click the **Silo Options** tab.
4. In the **Number of Silos to be kept in cache** box, type or select the number of dedicated data streams you want to change. The default value is set to 1.
5. Select **Enable Space Management** check box.
6. Click **OK**.



☑ Enable Backup of Deduplicated Data

☐ Archive Sealed DDB

☑ Number of Silos to be kept in cache 1

☑ Enable Space Management

Number of Silo streams 1

Amount of Data Size Moved: 1.85 GB

Amount of Data Size to be Moved: 30 MB

☐ Enable Multiplexing

Silo Archive Mux Factor: 1

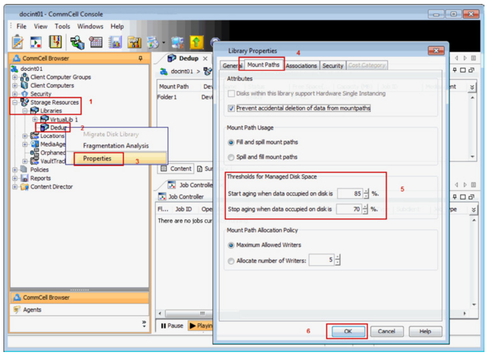
Select MediaAgent for Silo Restores docint01.testlab.comm...

Select Destination client for Silo Restores docint01.testlab.comm...

Add Data Path for Silo: Add Data Path

Use the following steps to set the thresholds on the disk:

1. From the CommCell Browser, navigate to **Policies** | **Storage Resources | *Library***.
2. Right-click the disk library and then click **Properties**.
3. Click **Mount Paths** tab.
4. The silo space management follows the disk space set in the **Thresholds for Managed Disk Space**.
5. Click **OK**.



Attributes

☐ Disks within this library support Hardware Single Instancing

☑ Prevent accidental deletion of data from mountpaths

Mount Path Usage

● Fill and spill mount paths

○ Spill and fill mount paths

Thresholds for Managed Disk Space

Start aging when data occupied on disk is 85 %.

Stop aging when data occupied on disk is 70 %.

Mount Path Allocation Policy

● Maximum Allowed Writers

○ Allocate number of Writers: 5

DISABLING SILO STORAGE

Once enabled, Silo Storage cannot be disabled from a storage policy copy. However, you can create a new Storage Policy without enabling silo storage and re-point the necessary Subclients to this Storage Policy.

REPORTS

MEDIA PREDICTION REPORT

The Media Prediction Report can be used to identify the backup tapes that are required for the Silo restore jobs. The following procedure provides the steps to run a Media Prediction Report:

1. From the CommCell Browser, click **Tools -> Reports...**
2. From the **Reports** pane, navigate to **Storage** and click **Media Prediction**.
3. Click **Run**.

SILO ARCHIVE JOB SUMMARY REPORT

The Silo Archive Job Summary provides job summary details of Silo archive jobs moving backup data from disk media to Silo Storage. The following procedure provides the steps to run a Silo Archive Job Summary report:

1. From the CommCell Browser, click **Tools -> Reports...**
2. From the **Reports** pane, click **Job Summary**.
3. From the **General** tab, click **Administrative Jobs** and then click **SILO Archiver**.
4. Click **Run**.

SILO RETRIEVE JOB SUMMARY REPORT

The Silo Retrieve Job Summary provides job summary details of retrieve job operations recalling data from Silo Storage. The following procedure provides the steps to run Silo Retrieve Job Summary report:

1. From the CommCell Browser, click **Tools -> Reports...**
2. From the **Reports** pane, click **Job Summary**.
3. From the **General** tab, click **Administrative Jobs** and then click **SILO Retrieve**.
4. Click **Run**.

LICENSE REQUIREMENTS

For Traditional License, the following licenses are required for Silo Storage:

- **Block Level De-Duplication** for deduplication of data on the disk media. This license is required on MediaAgents hosting the Deduplication Store.
- **Tape De-Duplication** license for providing the Silo Storage feature. This license is required on MediaAgents hosting the Deduplication Store.
- **GridStore** license for the additional data path required for Silo Storage.
- **FileSystem** license on the CommServe computer for creating Silo Storage.
- **FileSystem** license on the MediaAgent computer for creating Silo Storage. (For Unix MediaAgents only)
- **Advanced File System *i*DataAgent Options** license to store and retrieve silo storage data.

For License Usage by Capacity, Data Protection Enterprise (for Backup) or Archive Enterprise (for Archive) license is required.

EFFECTS OF OTHER OPERATIONS ON SILO STORAGE

Review the following consideration when using Silo Storage:

OPERATION	**DESCRIPTION**
Cloning Storage Policies	Storage Policies with silo-enabled copies cannot be cloned.
Look-Ahead Reader	Look-Ahead Reader operation is not applicable for Storage Policies with Silo enabled copies.
Spool Copy	Silo-enabled Storage Policy Copies cannot be configured as Spool Copies.
VaultTracker for Silo Storage	Data migrated to offsite storage using Silo Storage, when required for restore operations, can be tracked and located using VaultTracker® feature. See VaultTracker® Feature for more information on using the feature.
Data Aging Operations	When an active Silo store has been sealed and moved to storage, all the backup jobs that went to that store must meet the retention rules (defined in their associated storage policy copy) for the store to become aged. Once all of the jobs have met their retention criteria, the entire store is considered ageable, and the Silo (tape) backup jobs are then aged. The tape designated for the Silo storage is then refreshed and available for re-use.
Extended Retention	Extended retention rules are not supported on Storage Policy Copies configured for Silo Storage. If you have existing Silo enabled Storage Policy Copies with extended retention it is recommended that you remove the extended retention settings; extended retention on some copies would block the silo storage tapes from getting recycled.

Back to Top

Auxiliary Copy

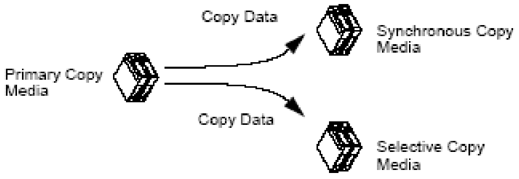
Topics | How To | Troubleshoot | How Do I | Support | Related Topics

OVERVIEW

An auxiliary copy operation allows you to create secondary copies of data associated with data protection operations, independent of the original copy. For a full understanding, you should have some basic knowledge of storage policy and storage policy copy configurations. See Storage Policies and Storage Policy Copies for more information.

The auxiliary copy operation can be useful for creating additional standby copies of data. The primary and secondary copies use different media and often use different libraries, depending on the configuration. Should the primary copy become inoperative, perhaps due to a storage media failure, or a library or network malfunction, you can promote a synchronous copy to become the primary copy. This allows you to continue operations as before and make repairs without interrupting data protection and data recovery operations.

When an auxiliary copy operation is started, all valid data from a source copy is copied to all or one active secondary copies within the storage policy. A source copy can either be the primary copy (the default), or a secondary copy that has been selected as the source copy. The following figure illustrates a primary copy as the source copy for an auxiliary copy operation:



- If the tape for a requested browse/data recovery operation is outside of a library, you will be prompted to manually input it into the library. The tape from a secondary copy will not be automatically used even if the data exists on the tape for the secondary copy.
- While performing Auxiliary Copy operations, priority is provided to perform the operation in a LAN-free environment.
- When auxiliary copy, data verification, and content indexing operations are initiated, they will all utilize the same single auxiliary copy manager process, thus reducing the load resources on the CommServe computer.

If a job is only partially copied, it can be recopied by using the **Re-Copy** feature. Doing this will re-copy all the chunks of the selected job from the beginning of the job. For more information, see Re-Copy Fully or Partially Copied Jobs.

DISABLING AND ENABLING A BACKUP JOB FOR AUXILIARY COPY

You have the ability to disable a backup job for the auxiliary copy, i.e., once a job is disabled, it will not be copied during an Auxiliary Copy operation. Additionally, if selected, those jobs that are dependent on the selected disabled job will be disabled as well.

Things to consider before you disable a job:

- A job that has been disabled can still be restored/recovered.
- If a primary copy has a disabled job, and during a data recovery operation the software cannot find any data, data from the disabled job will be used.
- If you disable a backup of the last cycle that has occurred, this forces the next backup to be a full backup.
- For the Exchange Database and Image *i*DataAgents, if you disable an incremental or differential backup, all subsequent backups will be disabled up to the next full backup.

For step-by-step instructions, see Disable/Enable a Job From a Storage Policy Copy.

AUXILIARY COPIES VS. STANDARD DATA PROTECTION OPERATIONS

An auxiliary copy should not be confused with a standard data protection operation. The two operations are unrelated, except, of course, that a data protection operation must precede an auxiliary copy. In all other ways the two operations are distinct and must be initiated or scheduled individually. A data protection operation is specific to a particular subclient, copying the subclient content from the client computer to the primary storage policy copy. An auxiliary copy, however, does not involve clients; instead, it copies backed up data from a source copy to one or more secondary copies. If you want the auxiliary copy operation to capture the data of only one subclient, then you must ensure that subclient has a dedicated storage policy.

AUXILIARY COPY AND HARDWARE COMPRESSION

Auxiliary copy does not manipulate software compression on the data. The data is transferred as it is. The hardware compression is transparent. Thus, hardware compressed data is uncompressed by the tape device on read, and recompressed during tape write.

AUXILIARY COPY AND MEDIA

If the media currently associated with your source copy is not readable or simply cannot be used, you can Disable/Enable All Jobs Associated with a Media so that all jobs associated with this media will be skipped during auxiliary copy operations.

If the media associated with the secondary storage policy copy becomes unreadable, you can Re-Copy all Jobs Associated with a Media. This will recopy all the jobs associated with the specific media.

AUXILIARY COPY WITH SYNCHRONOUS AND SELECTIVE COPIES

An auxiliary copy operation copies valid data from a source copy of a specific storage policy to all or one active secondary copy within a storage policy. Data from source copies are not copied over to inactive secondary copies.

These secondary copies can be either synchronous or selective copies. The following sections describe how data is copied during an auxiliary copy job on both types of copies.

SYNCHRONOUS COPIES

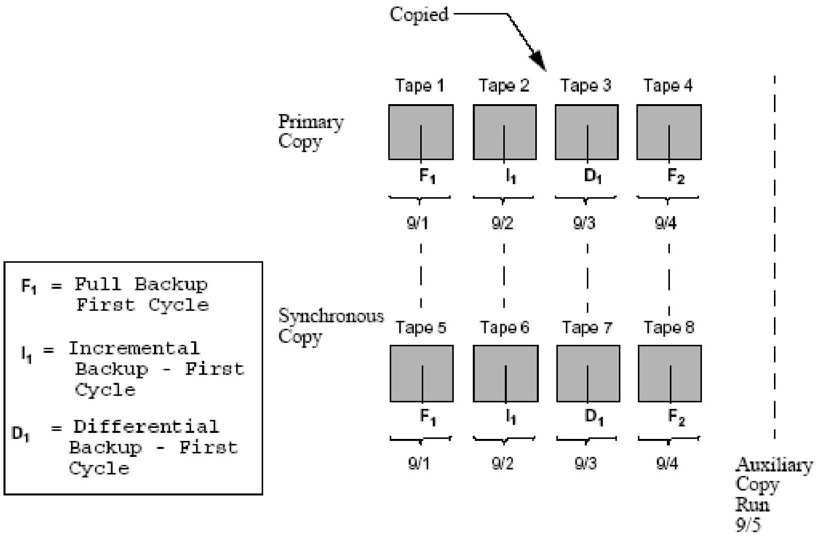
The auxiliary copy operation will copy full, incremental, and differential backup data from a source copy to other synchronous copies based on the `All Backups` option or the `Backups On And After` date you selected from the `Copy Policy` tab of the `Copy Properties` dialog box.

> If a primary copy has the Spool Copy (no retention) option enabled, and there is no coverage for all of the subclients in the secondary copies, the synchronous copy cannot be deleted. Instead, users will be prompted with a message to change the retention period of the primary copy or create another synchronous copy.

ALL BACKUPS OPTION

If you select the `All Backups` option when creating a synchronous copy, all data protection operations on a source copy will be copied to the synchronous copy.

In the following example, if an auxiliary copy is run on 9/5, F_1, I_1, D_1, and F_2 will be copied to the synchronous copy. The source copy for the operation is the primary copy.



When the `All Backups` option is selected, all data protection operations on a source copy will be copied to the synchronous copy.

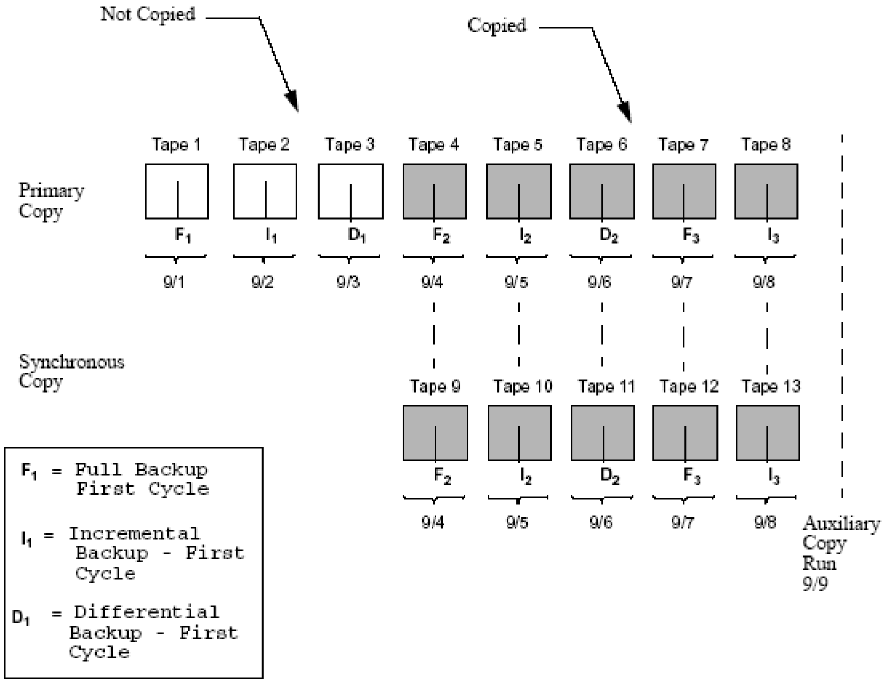
> When auxiliary copies are run on storage policies used by DataArchiver Agents, all archiving operations will be copied, regardless if a new Index exists.

BACKUPS ON AND AFTER OPTION

If you select a date from the `Backups On and After` field, then all data protection operations on or after the date you select, starting from 12:00 A.M., will be copied to the synchronous copy. This option is useful if you do not want all the data protection operations of a source copy to be copied to the synchronous copy.

Note that the date entered can be on, before, or after the current CommServe date. When the date entered is after the current CommServe date, jobs (up to the date specified) that are to be copied, as well as partially copied jobs will be disabled for copy. If no date is entered, all backup data will be copied from the primary copy to the secondary copy.

In the following example, the `Backups On and After` date was set to 9/4. All data protection operations starting from 9/4 are copied to the synchronous copy when an auxiliary copy operation is run on 9/9. All data protection operations prior to 9/4 are not copied.



When you enter a date that is earlier than (before) the date already specified, all data protection operations after the date specified or after the first copied/selected job, whichever is later, will be copied to the secondary copy.

For example, let's assume the current date is `January 1, 2009`, and you created a storage policy copy with the **Backups On and After** option set to `January 1, 2010`. This would indicate that all jobs up to `January 1, 2010` would be disabled for copy. With this, you manually pick a job for copy on `May 1, 2009`. On `June 1, 2009`, you revise the Storage Policy Copy **Backups On and After** option to be `January 1, 2009`. This will automatically select all jobs that are run after `May 1, 2009` (the first copied job), for auxiliary copy. Any jobs that were run before `May 1, 2009` would not be copied (in this scenario). To copy job(s) from any date before `May 1, 2009`, manually select the job(s) for copy. If you had not selected any job manually and modified the **Backups On and After** to `January 1, 2009`, all jobs from `January 1, 2009` to current date would have been picked up for auxiliary copy.

SELECTIVE COPIES

Selective copies only contain full backup data that has occurred on or after a specified date and are copied based on the following selective criteria:

- **Automatically select Full Backups** (`all`).
- **Automatically select Full Backups** (`weekly`, `monthly`, `quarterly`, `half yearly`, or `yearly`). This is a **time-based** Selective copy.
- **Do not Automatically select jobs**

The selective copy type can be selected from the `Selective Copy` tab of the `Copy Properties` dialog box. Once you set the `Backups On and After` date from the `Copy Properties` dialog box, then all data protection operations starting on or after the date you select (starting from 12:00 A.M.) will be copied to the selective copy, based on the selective copy type.

ALL FULLS BACKUPS

If a selective copy is defined as an `All Full Backups` copy, all full backups associated with the storage policy are copied to the selective copy.

TIME BASED SELECTIVE COPY

If a selective copy is defined as time based, an auxiliary copy operation copies the first or last full backup of a time period based on the following parameters:

Weekly The first or last full backup of a specified starting day of a week will be copied from 12:00 A.M. of that day up to 11:59 P.M. on the last day of that week.

Monthly The first or last full backup of a specified starting day of a month will be copied from 12:00 A.M. on that day up to 11:59 P.M. on the last day of that month.

Quarterly The first or last full backup of the first day of a quarter will be copied from 12:00 A.M. on that day up to 11:59 P.M. on the last day of that quarter.

Half Yearly The first or last full backup of the first day of a half year will be copied from 12:00 A.M. on that day up to 11:59 P.M. on the last day of that half year.

Yearly The first or last full backup of the first day of a year will be copied from 12:00 A.M. on that day up to 11:59 P.M. on the last day of that year.

Advanced This option allows you to select the First or Last full backup performed after a specific time period. The time period can be specified in cycles/days/weeks/months.

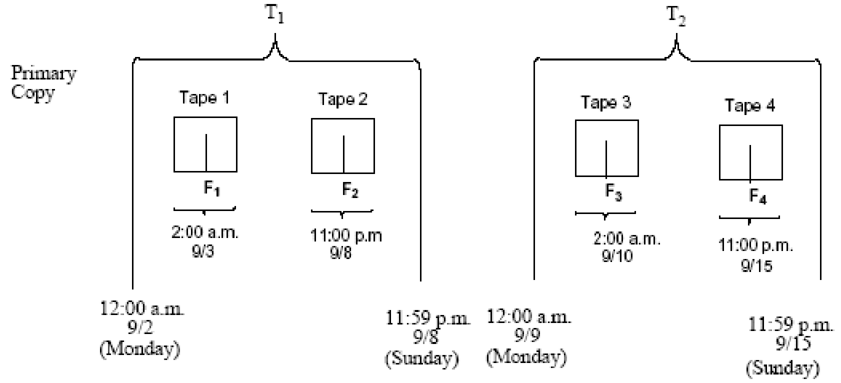
Note that for cycle based criteria, the copy selection is based on the mod logic. For more information, see For Selective Copy, how does the job selection work with Advanced - cycle based criteria?

A backup job will be selected based on its start time. For example: If a backup job starts at 11:55 pm on August 31st and ends at 1 am on September 1st, then it will be selected as the last full backup for the month of August.

Selective storage policy copies associated with custom calendars will have data copied during auxiliary copy operations monthly, quarterly, half yearly, or yearly based on the days defined in the calendar. See Custom Calendar for more information.

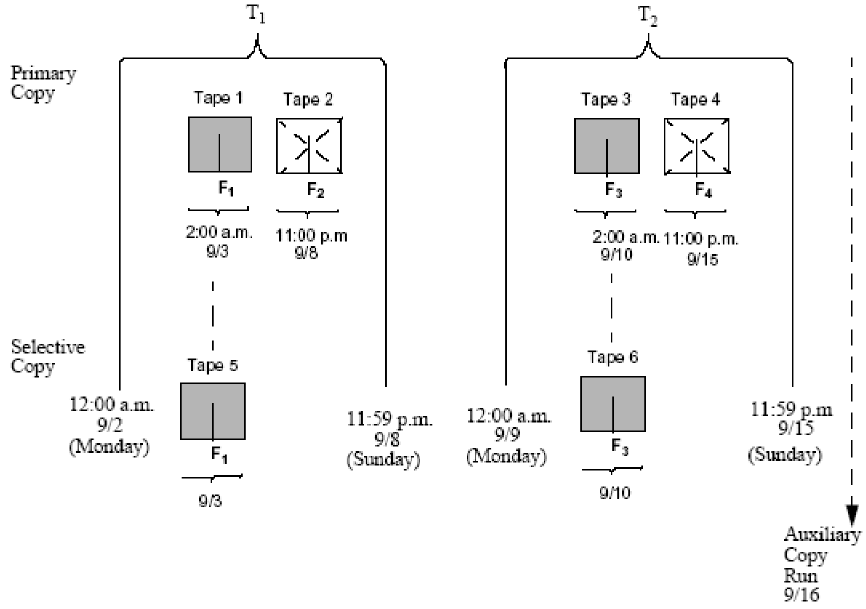
Example

The following example illustrates the time interval of a primary copy with four full backups that were run across two weekly time intervals, T_1 and T_2, every one week starting on Monday.



In the following example, a time based selective copy was specified as every one week starting on Monday, with the `First full backup` option enabled on the copy. Data protection operations were run across two time intervals on the primary copy, T_1 and T_2.

If an auxiliary copy operation is run on Monday 9/16, the first full backup within each weekly time interval (F_1 and F_3) will be copied to the selective copy.



If the `Last full backup` option is enabled on the copy instead of the First full backup option, then F_2 and F_4 will be copied instead of F_1 and F_3.

DO NOT AUTOMATICALLY SELECT JOBS

If a selective copy is defined as a `Do Not Automatically Select Jobs` copy no backups will be copied to this copy unless they are manually selected for copy from the Job for Storage Policy Copy dialog box or the **Select most recent full backup when auxiliary copy starts** option has been selected from the Auxiliary Copy Options dialog box.

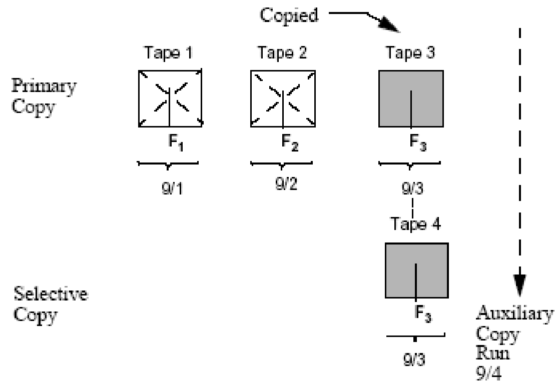
MANUALLY SELECT FULL BACKUPS

You can manually select a backup to be copied to a selective copy from the `Backups for Copy` window of the selective copy. See Manually Select a Backup To be Copied to a Selective Copy for more information.

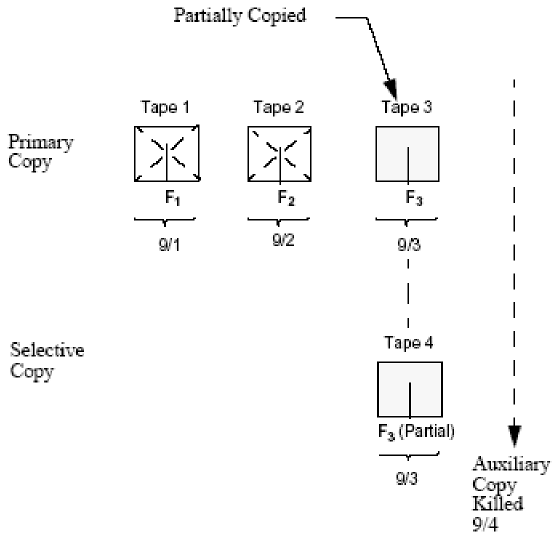
MOST RECENT FULL BACKUP SELECTIVE COPY

If you enable the **Select Most Recent Full Backup when Auxiliary Copy Starts** option when you initiate the auxiliary copy operation in the Auxiliary Copy (Options) dialog box, by default, when the auxiliary copy starts, the most recent full backup of each subclient, including those partially copied, and the previously selected full backup for each subclient will be copied.

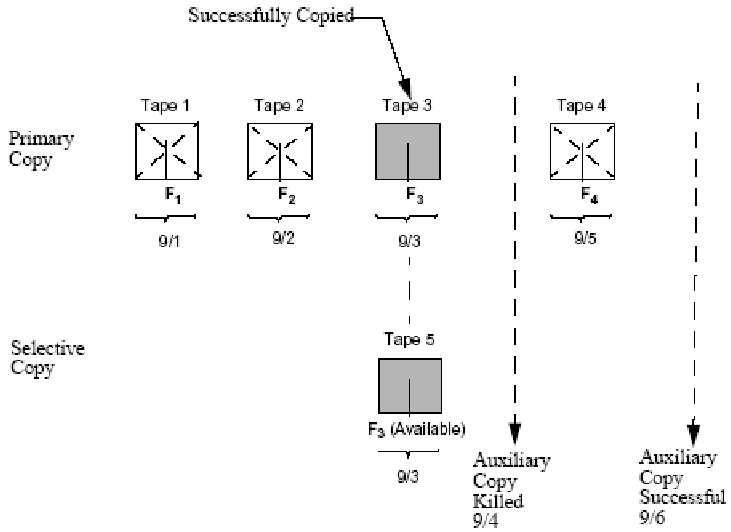
In the following example, three full backups are on the primary copy, F_1, F_2, and F_3. When an Auxiliary Copy is run on 9/4, F_3 will be copied because it is the most recent full backup.



In another example, if the same auxiliary copy is run on 9/4, but is killed before it is completely copied, F_3 may only be partially copied or selected for copy.



If another full backup (F_4) occurs on 9/5, and an auxiliary copy is run on 9/6, the partially copied full backup F_3 as well as F_4 will be copied. If while configuring the Auxiliary Copy Job, you disable the **Select Most Recent Full Backup When Auxiliary Copy Starts** option in the Auxiliary Copy (Options) dialog box, only the previously selected backup will be copied, thus F_4 would not be copied.

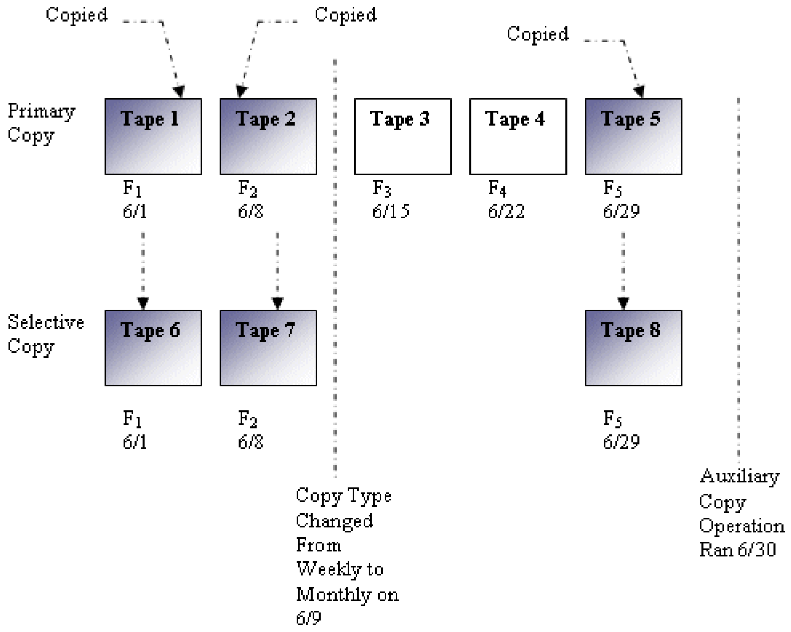


CHANGING THE SELECTIVE COPY TYPE OR SELECTIVE CRITERIA

If you change the selective copy type or selective criteria and then run an auxiliary copy operation, the auxiliary copy operation will copy the data based on the old and new selective copy criteria.

In the following example, on 6/9 the criteria of a selective copy was changed from being weekly based to monthly based.

If an auxiliary copy is run on 6/30, F_1 and F_2 are copied because they meet the weekly based criteria. F_5 is also copied because it meets the monthly based criteria.



Auxiliary Copy and Other Copy Features

The section describes how auxiliary copy is performed on copies that have other copy features enabled, such as:

- Combined Streams
- Inline Copy
- Deferred Copy

AUXILIARY COPY WITH DEFERRED COPIES

An auxiliary copy operation on a copy that has the `Defer Auxiliary Copy for <n> day(s)` option enabled, data will be copied starting at 12:01 A.M. on the set number of days after valid data becomes available on the source copy. See Deferred Copy for an overview.

AUXILIARY COPY AND SPOOL COPIES

An auxiliary copy must be performed on a primary copy that has the Spool Copy (no retention) option enabled, before data on that copy can be pruned the next time data aging is run. It is recommended that regular or automatic auxiliary copy operations are performed for storage policies using spool copies. See Spool Copy for an overview.

> Spool Copy data are aged upon the successful completion of the auxiliary copy job. If a primary copy has the Spool Copy (no retention) option enabled, and there is no coverage for all of the subclients in the secondary copies, the synchronous copy cannot be deleted. Instead, users will be prompted with a message to change the retention period of the primary copy or create another synchronous copy.

AUXILIARY COPY AND INLINE COPIES

If a data protection operation of a subclient whose storage policy has an inline copy enabled does not successfully create an Inline Copy, then the data will be copied to a secondary copy the next time an auxiliary copy is run. See Inline Copy for an overview.

AUXILIARY COPY AND PARALLEL COPIES

If storage policy copies are configured with an auxiliary parallel copy, after reading the source copy (only once) data can be copied to multiple secondary copies concurrently rather than sequentially. This optimizes use of media, therefore, decreases the time needed to run auxiliary copy operations. For more information, see Parallel Copy.

AUXILIARY COPY AND DEDUPLICATION

If a secondary storage policy copy is enabled with deduplication, then the deduplication store gets created for the copy and the associated data is deduplicated for that copy. See Deduplication for an overview.

- Data in a storage policy copy enabled for Deduplication can not be multiplexed. Therefore, Data Multiplexing is not supported if the storage policy copy is enabled with Deduplication. However, a SILO copy supports Data Multiplexing even if the storage policy copy is enabled with Deduplication.
- Multiplexed data cannot be copied to a storage policy copy enabled for Deduplication. Therefore, a storage policy copy enabled for Deduplication can not have a direct or indirect source copy enabled for Data Multiplexing.
- An Auxiliary Copy can be configured with Data Multiplexing when the source copy is enabled for Deduplication.

For more information, see Data Multiplexing.

DASH COPIES

When both primary copy and secondary copy are deduplicated, you can reduce the copy duration using the DASH Copy feature on the source computer while creating secondary copies. To optimize the disk read operations, enable the **Disk Read Optimized** Copy.

If you wish to process the signature on the source, to see if the signature is present on the target, and if present, send only the signature, you can enable **Network Read Optimized Copy**.

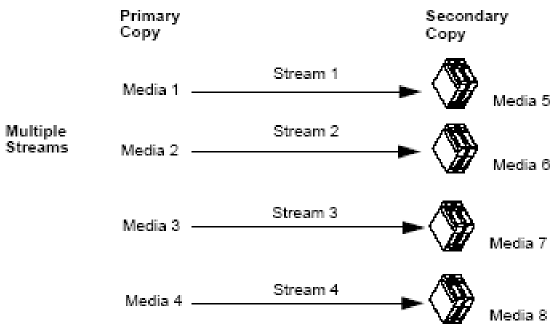
For more information, see DASH Copy.

AUXILIARY COPY WITH COMBINED STREAMS

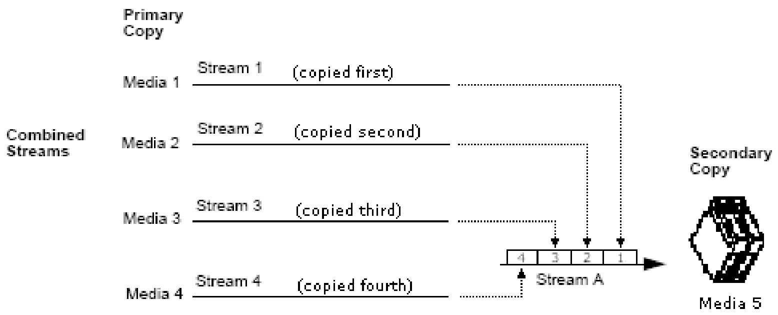
Auxiliary Copy normally copies data stream by stream, meaning, if there were four data streams on the primary copy, then the auxiliary copy operation would use four data streams to copy on the secondary copy. Alternatively, auxiliary copy can copy data from a primary copy that has multiple streams to a secondary copy that has less than that number of streams, by using the `Combined to <n> Streams` option on the copy.

By combining the data streams to less media, this improves media usage as the media storage is optimized. Media recycling is also more efficient, as data aging is more effective as secondary copies of the data reside on less media than what was required for the original data protection operation. The following example illustrates an auxiliary copy operation performed for a copy that combined data streams into one stream:

Secondary Copy Without Combined Streams



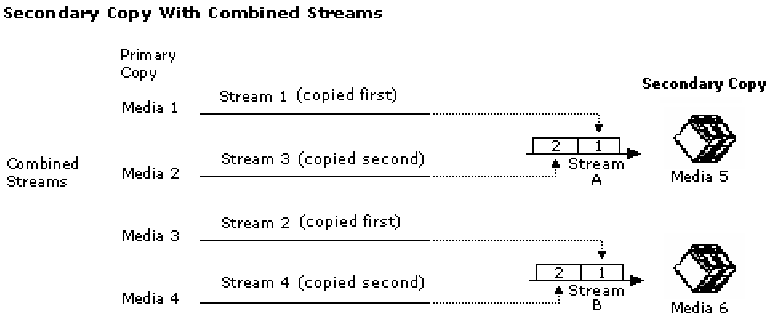
Secondary Copy with Combined Streams



Multi-stream backups of the Microsoft SQL, DB2, DB2 DPF and Sybase agents will be copied during an auxiliary copy operation to a copy that combines streams; however, restore operations may have limitations. See Browse and Restore for more information.

In order to restore SQL, DB2, DB2 DPF and Sybase agent backups from combined streams of Storage Policy copies, a new Storage Policy copy to disk library must be created and an auxiliary copy should be executed. A restore must be performed from this new copy.

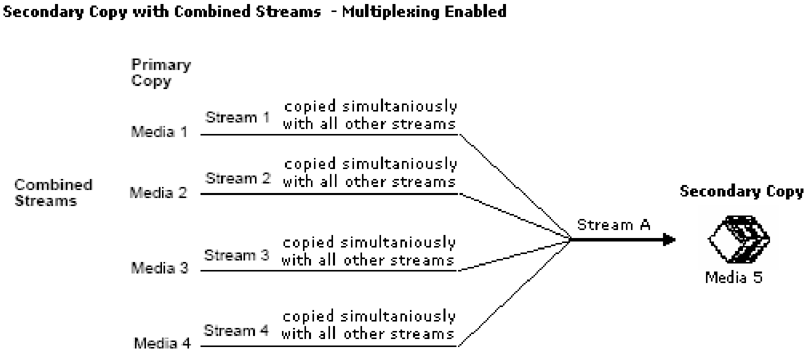
The following example illustrates an auxiliary copy operation performed for a copy that combined data streams into two streams:



Data Multiplexing

When a copy is configured to combine streams, thereby utilizing less media when copying data to a secondary copy, multiplexing can be enabled as well. Data Multiplexing allows data protection operations of multiple data streams to be run concurrently to the same media, which optimizes performance of the auxiliary copy operation in a disk environment.

The following example illustrates an auxiliary copy operation performed for a copy that combined data streams into one stream with multiplexing enabled:


Secondary Copy with Combined Streams - Multiplexing Enabled
Primary Copy
Media 1
Stream 1
copied simultaniously with all other streams
Combined Streams
Media 2
Stream 2
copied simultaniously with all other streams
Media 3
Stream 3
copied simultaniously with all other streams
Media 4
Stream 4
copied simultaniously with all other streams
Stream A
Secondary Copy
Media 5

For more information, see:

- Combine the Data Streams of a Storage Policy Copy
- Enable Multiplexing for a Storage Policy Copy with Combined Data Streams

  - Data in a storage policy copy enabled for Deduplication can not be multiplexed. Therefore, Data Multiplexing is not supported if the storage policy copy is enabled with Deduplication. However, a SILO copy supports Data Multiplexing even if the storage policy copy is enabled with Deduplication.
  - Multiplexed data cannot be copied to a storage policy copy enabled for Deduplication. Therefore, a storage policy copy enabled for Deduplication can not have a direct or indirect source copy enabled for Data Multiplexing.
  - An Auxiliary Copy can be configured with Data Multiplexing when the source copy is enabled for Deduplication.

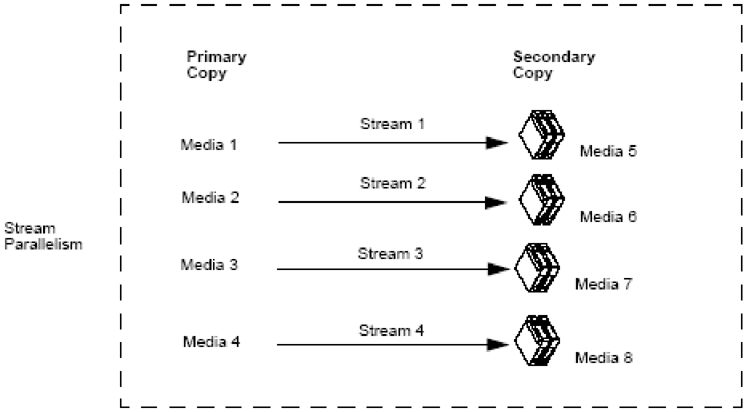
AUXILIARY COPY WITH MULTIPLE STREAM PARALLELISM

You can select the number of data streams to be copied at the same time during an auxiliary copy operation. This can be achieved by using the maximum number of available streams or from a specified number of streams.

ALLOW MAXIMUM NUMBER OF STREAMS OPTION

If enough storage resources are available, you can use the `Allow Maximum` option so that all data streams are copied concurrently during an auxiliary copy operation.

For example, if four streams were required for the auxiliary copy job, then all four streams will be copied in parallel.



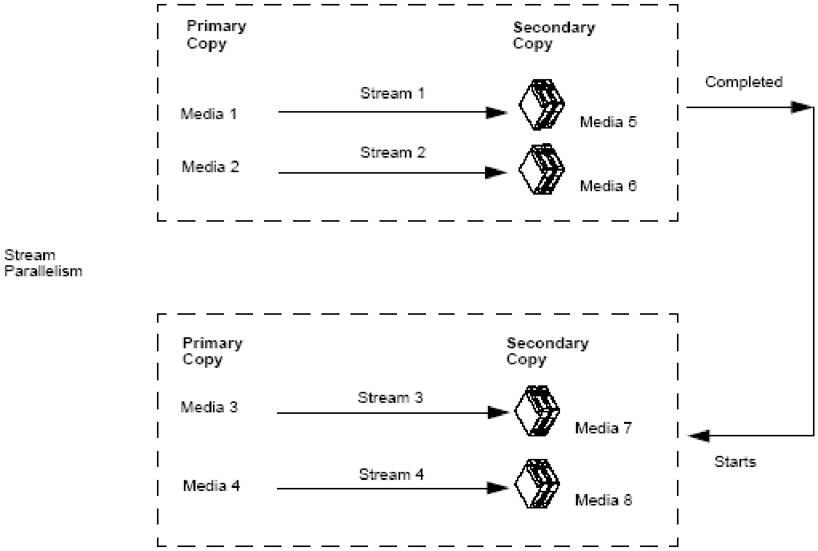
Data balancing occurs across multiple streams so that an auxiliary copy will continue to copy in parallel. Note that multiple streams will not be copied in parallel to a copy that combines streams.

- If an auxiliary copy is configured to copy with parallel streams, and the associated storage policy copy is configured with combined streams, the auxiliary copy operation will attempt to use no more than the number of streams defined in the storage policy copy's `Combined to n streams` field.
- Auxiliary Copy operations only use streams to perform copies of jobs with a "to be copied" status. Therefore, all available streams may not be used when performing an auxiliary copy.

LIMIT TO NUMBER OF STREAMS OPTION

If not enough storage resources are available, or you do not want to use all available resources, you can select the number of data streams that will be copied at the same time during an auxiliary copy operation.

For example, if four streams were required for the auxiliary copy job, and two streams are selected to copy in parallel, then the auxiliary copy operation will copy two streams at a time. Note that `Stream 3` will start when `Stream 1` or `Stream 2` is completed. Hence, `Stream 3` does not have to wait for both `Stream 1` and `Stream 2` to complete before starting.



STREAM RANDOMIZATION

When a storage policy is configured to use more than one data stream, it is important that the data streams are equally used; parallel copying using multiple source and destination drives may not be effective if the data is concentrated in one stream. The stream randomization feature enables random choosing of the data streams, increasing the rate of data transfer by copying data from different streams in parallel. See Enable Stream Randomization for instructions.

Also, it is recommended that you configure the tuning parameters to evenly distribute the data across all the streams. You can specify the interval to check the data size in the streams and the threshold to decide data distribution among the streams. See Tune Stream Randomization for instructions.

AUXILIARY COPY WITH A SPECIFIED SOURCE MEDIAAGENT

An auxiliary copy operation copies valid data from a specified source copy of a specific storage policy to all or one active secondary copy within a storage policy. If the source copy for the auxiliary copy operation is configured with a shared library, you will have the ability to select the source MediaAgent from which the auxiliary copy operation will read the data.

- All configured MediaAgents are displayed as options for the source MediaAgent. If an invalid MediaAgent is selected as the source for the copy, i.e., the source copy is not configured with the selected MediaAgent, the auxiliary copy operation will not produce the corresponding secondary copy, and the job may fail. Therefore, if the source copy for the auxiliary copy operation is not configured with a shared library, do not select a source MediaAgent for the operation; leave the field blank.
- An auxiliary copy operation configured with a source MediaAgent cannot be included in a **Schedule Policy** or the **Save As Script** feature.

For step-by-step instructions, see Select a Source MediaAgent for an Auxiliary Copy Operation.

AUXILIARY COPY OPERATIONS

You can start or schedule an auxiliary copy at the storage policy level from the Auxiliary Copy (Options) dialog box.

From this dialog box, you can:

- Select the Source MediaAgent from which this auxiliary copy operation will be performed. (Only if source copy is configured with a shared library.)
- Copy the data to all secondary copies.
- Copy the data to a specific secondary copy.
- Start new media for all secondary copies.
- Mark a media full after a successful operation.
- Select a number of streams to copy in parallel.
- Select vault tracking, change priority, start suspended.
- Specify Job Running Time, and Job Restart interval options. (You can also specify the maximum number of allowed restart attempts and the interval between restart attempts for all auxiliary copy jobs. For procedures, see Specify Job Restartability for the CommCell.)

Additionally, from the Auxiliary Copy (Job Initiation) dialog box, you can schedule the auxiliary copy operations that you configured.

From this dialog box, you can:

- Run the auxiliary copy operation immediately.
- Schedule the auxiliary copy operations via the Schedule Details dialog box.
- Save the operation as a script.
- Set an Automatic Copy schedule: The auxiliary copy operation will be performed every 30 minutes, unless another interval has been specified. See Automatic Copy for more information.
- Configure an alert for the operation.

SEQUENCE IN WHICH DATA IS COPIED DURING AN AUXILIARY COPY OPERATION

Data is copied to secondary copies during auxiliary copy operations according to the media of the original data protection operations, per destination copy and data stream. More specifically, the media that contains the oldest job is copied first. From this media, jobs from the primary copy are copied sequentially from oldest to newest so that all jobs from this media are copied before unmounting it. Once all the jobs are copied from this media, auxiliary copy will continue with the next media containing the oldest job within the same drive pool. When all the media in this drive pool are copied, auxiliary copy will start copying the oldest media of the other drive pools that belong to the same library. When all the media in this library are copied, auxiliary copy will continue copying the oldest media of the other libraries for the same MediaAgent. When all the media of this MediaAgent is copied, auxiliary copy will start copying the oldest media of other MediaAgents. Upon completion, if there is more than one stream, auxiliary copy will continue copying on the next stream in the same manner. Therefore, data is copied in the following sequence:

- Media

  For example, J_1 and J_2 used media M_1. J_3 and J_4 used media M_2. J_1 and J_2 are copied first, and then J_3 and $J_{4.}$

- Drive Pool

  For example, J_1, $J_{2,}$ J_3 and J_4 used drive pool D_1. J_5, $J_{6,}$ J_7 and J_8 used drive pool D_2. J_1, $J_{2,}$ J_3 and J_4 are copied first grouped by media and volume. J_5, J_6, J_7 and J_8 are copied second.

- Library

  For example, J_1 and J_3 used library L_1, and J_2 and J_4 used library L_2. J_1 and J_3 are copied first grouped by media and volume. J_2 and J_4 are copied second.

- MediaAgent

For example, J_1, J_2, J_3, J_4, J_5, J_6, J_7, and J_8 use MediaAgent MA_1. J_9, J_{10}, J_{11}, J_{12}, J_{13}, J_{14}, J_{15}, and J_{16} use MediaAgent MA_2. J_1 through J_8 are copied first grouped by media, volume, and drive pool. J_9 through J_{16} are copied second.

See View the Media Not Copied for step-by-step instructions.

CHANGE JOB PRIORITIES TO COPY DURING AUXILIARY COPY OPERATION

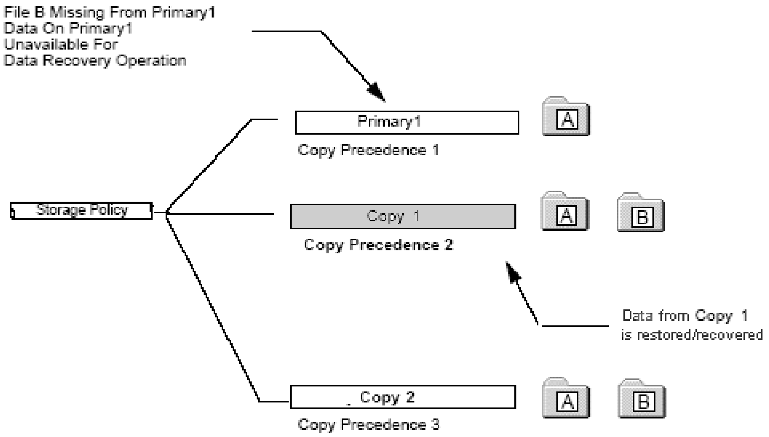
When Auxiliary Copy operation is performed, jobs (data) from primary copy to secondary copy are copied sequentially from oldest to newest jobs. During this process, you can set the priorities for jobs to be copied to secondary storage. See Set Job Priorities to Copy during Auxiliary Copy operation for step-by-step instruction.

RECOVERING DATA FROM COPIES

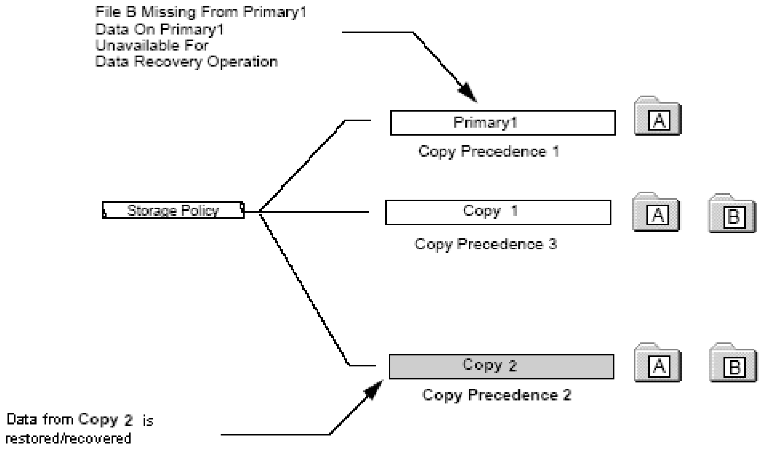
By default, when a browse or data recovery operation is requested (without specifying copy precedence), the software attempts to browse/restore/recover from the storage policy copy with the lowest copy precedence. If the media for the copy with the lowest precedence is offsite, damaged, or if hardware resources are unavailable, then a specific storage policy copy must be specified in the Copy Precedence tab of the **Storage Policy Properties** dialog box. For more information, see Change the Copy Precedence.

If the data that you want to browse/restore/recover was already pruned from that copy, the software will search for the requested data from a copy with the lowest copy precedence number to copy with the highest copy precedence number.

In the following example, a storage policy includes three copies, a primary copy (with copy precedence 1) and two additional copies. If File B is unavailable from the primary copy, then, when performing a data recovery operation, data will automatically be restored/ recovered from `Copy1` that has a copy precedence of 2.



If, however, the copy precedence of the two copies was changed so that `Copy 1` has a copy precedence of 3 and `Copy 2` has a copy precedence of 2, then the data recovery operation will be performed from data obtained from `Copy 2` that has a copy precedence of 2.



BROWSE/RESTORE/RECOVER FROM COPY PRECEDENCE

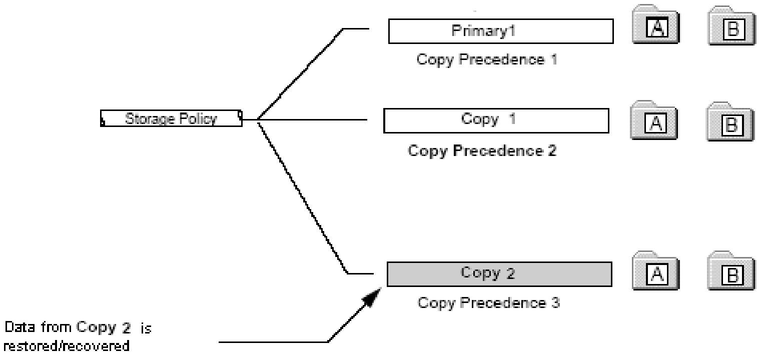
When a copy is configured, the system automatically assigns it a copy precedence number, which you can change at any time.

If you specify a copy precedence number for a data recovery operation, the software searches only the storage policy copy with that precedence number in each of the storage policies through which the data was secured. If data does not exist in the specified copy, the data recovery operation fails even if the data exists in another copy of the same storage policy.

Copy precedence is useful if:

- The primary copy is no longer available for a data recovery operation due to a hardware failure.
- You know that the media containing the data from data protection operations for a particular copy have been removed from the storage library. In this case, you can choose to browse/restore/recover from a copy whose media are inside the library.
- You want to browse/restore/recover from a selective copy.
- You want to browse/restore/recover from a copy that accesses faster disk media rather than slower tape media.
- You know that the media drives used by a particular copy are busy with another operation and want to browse/restore/recover from a different copy to avoid resource conflicts.

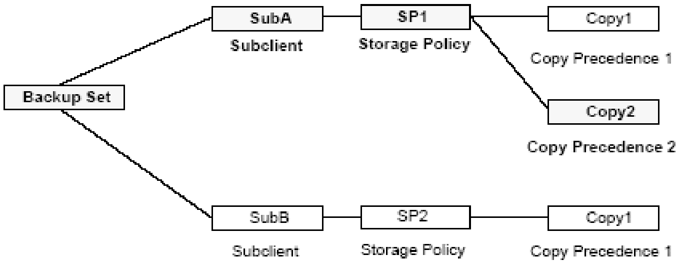
In the following example, a storage policy has a primary copy, Primary1, two copies, `Copy 1`, and `Copy 2`. If you choose to browse/restore/recover your data from `Copy 2`, you must specify that you want to browse/restore/recover from copy precedence 3 so that data will be restored/recovered from that copy.



BROWSING FROM COPY PRECEDENCE ACROSS MULTIPLE STORAGE POLICIES

When you browse at the client, agent, or backup set levels, keep in mind that the data for the subclients included in these levels may have been secured through more than one storage policy. If you specify a copy precedence for a data recovery operation, the data is restored/recovered from the storage policy that has data on the specified copy.

For example, data is restored/recovered at the backup set level that has two subclients, `SubA` and `SubB`. `SubA` uses storage policy `SP1` and `SubB` uses storage policy `SP2`. `SP1` has two copies, `Copy1` and `Copy2`. `Copy1` has a copy precedence of 1, and `Copy2` has a copy precedence of 2. If copy precedence 2 was selected for the data recovery operation, only data from SubA will restored/recovered.



RESTORING DATA FROM A SECONDARY COPY USING A THIRD-PARTY COMMAND LINE

The Oracle, SAP for Oracle, and SAP for MAXDB *i*DataAgents provide the capability of restoring data from secondary copies using a third-party command line, such as RMAN and the SAP command line. Using a third-party command line for this operation provides an alternative to the CommCell Console, and is useful for restoring data when the primary copy is unavailable. To utilize this feature, some minor setup configuration is required depending on the agent, as described briefly below:

- For Oracle, the setup involves adding the **`PARMS="ENV=(CV_restCopyPrec=2)"`** parameter statement into the RMAN restore script.
- For SAP for Oracle or SAP for MAXDB, the setup consists of adding the **`CV_restCopyPrec`** parameter followed by the copy precedence number **`2`** into the

parameter file prior to running the restore.

See Restore Data from a Secondary Copy using a Third-Party Command Line for step-by-step instructions.

Safeguarding Your Data Using Auxiliary Copy With Selective Copies

You can use the Auxiliary Copy feature to copy your data to selective copies, and then use the Export Media option to keep these copies of your data in a safe offsite location. By defining your selective copy to contain one full backup in a three month period, and by using the `Export Media` option, you can guarantee that you can keep a secondary copy of full backup data every three months in a safe location. This provides for extra protection in the event of data loss.

To accomplish this:

- Create a Selective Copy
- Schedule an Auxiliary Copy

  To guarantee that data will be copied to the selective copy you have defined, create an Auxiliary Copy schedule. This schedule will dictate when the full backup(s) will be copied from the primary copy to the selective copy media. If resources permit, create a schedule to run every day, for example, every day at 9:00 A.M. New, eligible full backups will be copied when the Auxiliary Copy operation is run. No drive resources will be used if no eligible full backups have occurred since the last Auxiliary Copy was performed for the Storage Policy.
- Perform an Export Media Operation Using Vault Tracker

  Once you have copied your data to selective copies using auxiliary copy operations, you can now export your media to keep it in a safe offsite location.
- Perform a Manual Export Based on a Report

  If you want to take the tapes out manually (either by opening the library door or through selecting a list), run the `Media Information` report. Based on the report, (which you can to run at the same frequency and options as above) the tapes may be manually exported.

Skip Job on Read Errors During Auxiliary Copy

The **Skip job on read errors during Auxiliary copy** option specifies whether the Auxiliary Copy job will skip data protection jobs that encounter errors during auxiliary copy operations. If you have many data protection jobs that need to be copied, this option will allow the auxiliary copy job to continue copying other data protection operations while skipping over those jobs encountering errors. This option is enabled by default. However, if you disable the option and the Auxiliary Copy job encounters an error, it will return with a Pending status and not continue. The **Skip job on read errors during Auxiliary copy** option can be modified from the Media Management Configuration (Auxiliary Copy Configuration) dialog box available in the Control Panel. If you continue to encounter errors, contact your software provider.

> **Pending** reasons are displayed in the **Reason for Job delay** field, which is located in the Administration Job Details (General) tab.

For more information regarding the effects if an error is encountered during auxiliary copy operations, please refer to the following table.

If The Following Error Occurs	**Then**
`Source Media Error/Source Media Not Available`	The auxiliary copy job will continue copying other data protection jobs while skipping over that media. Upon completion of all jobs that need to be copied, the jobs on the skipped media will be attempted to be copied again. Note that when it skips the media â€" it skips all the jobs on that media. If the first source media is not available, wait.
`Read Error`	The auxiliary copy job will continue copying data protection jobs while skipping over the portion of the job with the read errors. Upon completion of all jobs that need to be copied, the skipped portions will be attempted to be copied again.
`Target Media Mount Error`	The auxiliary copy job will retry the operation. If error still exists, the job will go into Pending state.

Auxiliary Copy Considerations

- Software compressed data is not uncompressed during an auxiliary copy operation.
- If you disable a data protection operation associated with a primary copy, that backup will not be copied during an Auxiliary Copy operation.
- Once started, if an auxiliary copy job cannot be completed, the Job Manager will retry the job up to a total of two days at 20-minute intervals for a maximum of 144 times.
- Multiple streams will not be copied in parallel to a copy that combines streams.
- To avoid possible media contention, which can affect performance, it is recommended that you do not start an auxiliary copy operation if the selected storage policy is already being used by a data protection or data recovery operation. To determine the jobs scheduled for a storage policy:
  - Identify the storage policy associated with a job, see the Storage Policy column of the Job Controller.
  - To view a list of jobs scheduled in the CommServe, click the CommServe icon or a specific storage policy, then select **View Schedules.**

- When defining the rules for a selective copy in the Copy Properties (Selective Copy) dialog box, it is recommended to select the **Select Full Backups at frequency** option. Selecting the **Copy most recent full backups when Auxiliary Copy starts** option will copy the most recent full backup of each subclient, including those partially copied, and the previously selected full backup for each subclient. For more information, see Most Recent Full Backup Selective Copy.
- The amount of data transferred for an Auxiliary Copy job is updated every 512 MB or when a data chunk is closed. The progress for the entire job is displayed on the Administration Job Details (General) tab, and the per copy progress is displayed on the Auxiliary Copy Job Details (Streams) tab. The data chunk size can be changed from the Media Management Configuration (Chunk Size) or storage policy copy's Data Path Properties dialog boxes.
- The priority of an auxiliary copy job can be changed using the Change Job Priority feature.
- Data paths can be added to secondary copies to enable LAN free Auxiliary Copy operations, so that network resources can be freed wherever possible. For more information, see Configuring Alternate Data Paths for Secondary Copies.
- An excessive number of concurrent read/writes may affect performance. For a single disk, a maximum of two (2) concurrent I/O streams is recommended. For a RAID 5 volume, a maximum of five (5) concurrent I/O streams is recommended.
- If the source copy is disk and managed by a Windows MediaAgent, enable the **Use Unbuffered I/O** option for each mount path. Use of unbuffered I/O can significantly improve performance. For more information, see Administering Mount Paths.
- If the default data path on the primary copy of a storage policy points to a drive pool configured on a MediaAgent enabled with NDMP Remote Server (NRS), then the secondary copy must also point to a drive pool configured on a MediaAgent with NRS installed in order to restore the data to a NAS file server.
- Only for EMC Celerra 5.5 must the library be directly attached to the Celerra file server. For EMC Celerra 5.6 or higher, when a Celerra file server is backed up using the Volume-Based Backup option, three-way backups, three-way restores, and NDMP Remote Server (NRS) are available. For this reason, you can perform an Auxiliary Copy operation that would copy a Volume-Based Backup to a library that is not attached to the Celerra file server, because it is possible to restore that data.
- Auxiliary copy operations will maintain the data format of multiplexed data. If not all of the multiplexed data is required by the auxiliary copy operation (e.g., destination copy is a Selective type), the auxiliary copy operation will perform slower as un-required data is read and discarded. For better performance, reduce the level of multiplexing. For more information, see De-Multiplexing Multiplexed Data.
- To prevent a job from being copied to the same library during auxiliary copy operations, select the **Write to a Different Library Compared to Source Copy** option in the Copy Properties (Media) dialog box.
- During auxiliary copy operations for Oracle instances, the job status may go pending if the RMAN delete command is initiated to delete pieces of the backup job being copied. This is because the auxiliary copy manager can no longer retrieve the archive file information created from the archive manager. The auxiliary copy operations will automatically resume; however, the oracle backup job will be copied to second copy without the deleted pieces, which makes the job unrecoverable.

Inline Copy

- The multiplexing factor of the primary storage policy copy will be automatically used as the multiplexing factor for the secondary storage policy copy.

Network Load

The Copy Properties (Data Path Configuration) dialog box includes the following options for auxiliary copy operations that will assist with controlling network load.

- **Use LAN Free MediaAgent Only** This option allows users to opt for a LAN Free MediaAgent (drive pool) to be used for auxiliary copy operations. Selecting this option reduces network load because data is not transferred across a network.
- **Throttle Network Bandwidth per stream (MB/HR)** This option allows you to reduce (control) the Auxiliary Copy throughput so that the entire network bandwidth is not consumed. By default, the value is set to 500 megabytes per hour per stream. Increasing this value increases the bandwidth consumption, while decreasing the value decreases the bandwidth consumption. Note that the auxiliary copy throughput is restricted to the maximum bandwidth on the network.

CUSTOMIZE AUXILIARY COPY OPERATIONS THROUGH REGISTRY KEYS

- Periodically, Auxiliary Copy operations update the status of the jobs that are currently being copied. By default the status will be updated every 60 minutes, as well as at the end of the Auxiliary Copy operation. The time interval for the status updates can be modified using the AUXCOPY_MARKCOPIED_MINUTES registry key.
- Auxiliary Copy operations copy all eligible data, even from data protection operations that have finished after the auxiliary copy operation has started. Auxiliary Copy operations can be prevented from copying this new data by configuring the AUXCOPY_NOT_PICK_NEW_BACKUPS registry key.
- Auxiliary Copy operations prune copied jobs from the spool copy every hour or upon completion. This can be modified using the AUXCOPY_NOT_PRUNE_SPOOL_COPY registry key. If defined and enabled, the auxiliary copy will not prune any job from the spool copy.
- You can enable the Auxiliary copy operations on migrated storage policies using the AUXCOPY_LOCAL_COMMCELL_ONLY registry key.

AUXILIARY COPY ENCRYPTION

While data encryption provides pass-phrase, key management, and network encryption support, you can also encrypt storage policy copies using auxiliary copy encryption. This capability allows you to select portions of data you wish to encrypt, does not require client encryption configuration, and provides faster encryption performance.

See Auxiliary Copy Operations and Encryption for more information.

SCHEDULING

Operations for this feature can be scheduled to run on a regular basis. To create a job-based schedule for this feature in your CommCell environment, see Create a Job Schedule.

If you have a large number of clients/backup sets/subclients, or storage policies in your CommCell that require the same schedule, it may be more beneficial to create a schedule policy for this operation; see Create a Schedule Policy.

BEST PRACTICES

ENABLE AND CONFIGURE THE AUXILIARY COPY FALLEN BEHIND ALERT

Configure the **auxiliary copy fallen behind alert** so that you are notified when the data to be copied for the associated storage policy exceeds the threshold and/or the number of days the jobs for the associated storage policy have not been copied exceeds the set threshold. The thresholds for this alert can be set in the Storage Policy Properties (Advanced) window. For more information, see Alerts: Job Management.

FREQUENTLY ASKED QUESTIONS

FOR SELECTIVE COPY, HOW DOES THE JOB SELECTION WORK WITH ADVANCED - CYCLE BASED CRITERIA?

On a Selective Copy, if you have selected **Automatically select Full Backups at frequency** option with **Advanced** - **Every <x> Cycle(s)** option, then the job selection will be done based on the Mod Logic.

The Mod Logic is implemented as follows:

N mod x

- If N mod x is 1 then only first full backup jobs will be selected.
- If N mod x is 0 then the last full backup jobs will be selected.

Where:

N - is the cycle number of a backup job as seen under **Cycles/Sequence** column in the **Job for Storage Policy/Storage Policy copy** window, which will appear by right-clicking the **Storage Policy**, pointing to **All Tasks** and then clicking **View Jobs**.

x - is the number of cycles defined in the **Every <x> Cycle(s)** option in the **Advanced Options** dialog box.

Example:

- If N = 3 and x = 2, then N mod x => 3 mod 2 = 1 - the backup will qualify as a first full backup.
- If N = 2 and x = 2, then N mod x => 2 mod 2 = 0 - which means that backup will qualify as last full backup for the copy, if last full backup option is selected.
- If you have specified **Every <x> Cycles (s)** values as 4 (i.e., x = 4) during selective copy creation and selected **First Full Backup** option and during copy creation if the number of backup cycles on a source copy is 16 (i.e., N = 16), then:
  - 16 mod 4 = 0 and this backup will not qualify as first full backup for this newly created selective copy as the mod value is 0.
  - If the backup cycle value is 17 (i.e., N = 17), then 17 mod 4 = 1, this backup will be qualified for copy as first full backup for this copy.

  In case of backup cycles N = 18, 19, 20 e.t.c., these backups will not qualify for copy selection because of mod logic.

CAN I COPY ALTERNATE CYCLE JOBS TO TWO DIFFERENT SELECTIVE COPIES?

If you wish to copy alternate cycle jobs (i.e., one odd and one even) to different copies then perform the following:

- Configure two selective copies.
  - On one copy, right-click the copy, and then click the Properties.

    In the **Selective Copy** tab, from the **Automatically select Full Backups at frequency** list select **Advanced.**

    In the **Advanced** dialog box select **Every <x> Cycles** and specify the value as **2**.

    Select **First Full Backup** option.

    Click **OK**.
  - On another copy, right-click the copy, and then click the **Properties**.

In the **Selective Copy** tab, from the **Automatically select Full Backups at frequency** list select **Advanced.**

In the **Advanced** dialog box select **Every <x> Cycles** and specify the value as **2**.

Select **Last Full Backup** option.

Click **OK**.

This allows you to copy the alternate cycles jobs to two different copies by implementing the mod logic explained in the above FAQ.

RELATED ALERTS

The following Job Management Auxiliary Copy alerts can be configured from the Alerts Wizard:

- Job Succeeded
- Job Skipped
- Job Failed
- Job Activity
- Auxiliary Copy fallen behind alert
  - The thresholds for this alert must be configured in the Storage Policy Properties (Advanced) window.
- Delayed by *n* Hrs
- Alert every *n* attempt (Phase failures)
- Alert every *n* attempt (Network failures)

For more information, see:

- Alerts: Job Management
- Configure Alerts

RELATED REPORTS

ADMINISTRATIVE JOB SUMMARY REPORT

The Administrative Job Summary Report displays a summary of all or select Administrative jobs.

AUXILIARY COPY JOB SUMMARY REPORT

The Auxiliary Copy Job Summary Report displays auxiliary copy jobs and associated details.

JOBS IN STORAGE POLICY COPIES REPORT

The Jobs in Storage Policy Copies Report displays the data protection jobs associated with the storage policy copies.

Back To Top

Auxiliary Copy - How To

Topics | How To | Troubleshoot | How Do I | Support | Related Topics

Recover Your Data From Copies

Restore Data from a Secondary Copy using a Third-Party Command Line (Oracle, SAP for Oracle and SAP for MAXDB *i*DataAgents)

Select a Source MediaAgent for an Auxiliary Copy Operation

Export Media Using Vault Tracker

Set Job Priorities to Copy during Auxiliary Copy operation

SCHEDULE AN AUXILIARY COPY

*Required Capability***:** See Capabilities and Permitted Actions

To schedule an auxiliary copy:

1. From the CommCell Browser, right-click the storage policy for which you want to perform an auxiliary copy, click **All Tasks**, and then click **Run Auxiliary Copy**.
2. From the Job Initiation tab on the **Auxiliary Copy** dialog box, select **Schedule**, and click **OK**.
   - From the Schedule Details tab, select the necessary scheduling options.
   - To view the job summary for the auxiliary copy job that you have scheduled, click the Job Summary tab.
3. Click **OK** to save the schedule.

START AN AUXILIARY COPY

Required Capability: See Capabilities and Permitted Actions

To start an auxiliary copy:

1. From the CommCell Browser, right-click the storage policy for which you want to perform an auxiliary copy, click **All Tasks**, and then click **Run Auxiliary Copy**.
2. In the **Auxiliary Copy** dialog box, the Storage Policy field is already populated with the name of the Storage Policy you selected.
3. If the source copy is configured with a shared library, select the **Source MediaAgent** for the auxiliary copy.
4. Select **All Copies** to copy data from the source copy to all secondary copies defined, or select a copy from the `Select a Copy` list box.
5. Select **Start new media** to copy the data to a different tape or optical media. On a disk, this option, when selected, creates a new volume folder for the operation.
6. Select the number of streams to copy in parallel from the **Number of Streams to Copy in Parallel** pane, or select **Allow Maximum**.
7. Select **Mark media full after successful operation** to mark the media that is used for this operation full after the auxiliary copy operation has successfully completed.
8. Select **Select Most Recent Full Backup When Auxiliary Copy Starts** to have the most recent successful full backup for each subclient copied when the Auxiliary Copy job is run.
9. From the Job Initiation tab on the **Auxiliary Copy** dialog box, select the time for this job to run or choose to **Run Immediately**. You can also configure an alert for this job.
10. Click **Advanced** to configure the **Vault Tracker**, **Startup** and **Job Retry** options.
    - Click **Vault Tracking** to select additional Vault Tracker options for this operation from the Vault Tracking dialog box.

      Note: This option is only available if a Vault Tracker license is available in the CommServe.
    - Click **Startup** to change the priority of this job and, if necessary, to start this job in a suspended state from the Startup dialog box.
    - Click the **Job Retry** tab to specify the job running time and the number of job retries. See Restarting Jobs and Job Running Time for more information.

      The **Number of Retries** specified for this particular job will only be used by the system if Auxiliary Copy was configured as a **Restartable** job type in the Job Management Control Panel. For procedures, see Specify Job Restartability for the CommCell.
11. Click **OK** to start the auxiliary copy operation. A progress bar displays the progress of the operation.

CREATE AUTOMATIC COPY SCHEDULE

Required Capability: See Capabilities and Permitted Actions

To create an automatic copy schedule:

1. Right-click the storage policy associated with the secondary storage policy copy for which you wish to enable Auxiliary Copy operations, and then click **Run Auxiliary Copy**. To configure the copy options, refer to Start an Auxiliary Copy.
2. From the Job Initiation tab of the **Auxiliary Copy** dialog box, select **Automatic Copy**, and if necessary, change the **Interval** time in which the copy should run; the default is set to every 30 minutes.

   You can set the time interval between 15 to 1440 minutes.
3. Click **OK** to save your changes.

DISABLE/ENABLE A JOB FROM A STORAGE POLICY COPY

Required Capability: See Capabilities and Permitted Actions

To disable a job associated with a primary copy:

1. From the right pane of the CommCell Browser, right-click the copy whose jobs you want to disable, click **View** and then click **Jobs**.
2. Select the necessary filter options in the Job Filter for Storage Policy Copy dialog box.
3. Click the **Advanced** button for additional filter options in the Jobs in Storage Policy Advanced Filter Options dialog box. Click **OK**.
4. A list of jobs associated with a storage policy copy is displayed in the Jobs for Storage Policy Copy window.
5. Right-click on a job, and click **Prevent Copy** (for primary copies) or **Do Not Copy** (for secondary copies).
   - To select multiple jobs, hold down the **Ctrl** key, and right click on the jobs.
6. Select whether you want to prevent the associated incremental jobs in the **Prevent Copy** dialog box.
7. A list of all jobs that will be disabled in addition to the job you selected are displayed in the Prevent Copy dialog box.
8. Click **OK**.
9. Click **Yes** on the Confirmation pop-up window.

To enable a job associated with a primary copy:

1. From the right pane of the CommCell Browser, right-click the primary copy whose jobs you want to disable, click **View** and then click **Jobs**.
2. Filter the necessary options in the Job Filter for Storage Policy Copy dialog box. Click **OK**.
3. A list of jobs associated with a storage policy copy is displayed in the Jobs for Storage Policy Copy window.
4. Right-click on a job, and click **Allow Copy**.
   - To select multiple jobs, hold down the **Ctrl** key, and right click on the jobs.
5. Click **Yes** on the Confirmation pop-up window.

DISABLE/ENABLE ALL JOBS ASSOCIATED WITH A MEDIA

Required Capability: See Capabilities and Permitted Actions

To disable all jobs associated with a media:

1. From the right pane of the CommCell Browser, right-click the copy containing the media to which you want to disable jobs, click **View** and then click **Media**.
2. From the Media List dialog box, right-click on the media for which you wish to disable jobs and select **Prevent Copy**.
   - To select multiple media items, hold down the **Ctrl** key, and right click on the media.
3. Click **Yes** on the Confirmation pop-up window.

To enable all jobs associated with a media:

1. From the right pane of the CommCell Browser, right-click the copy containing the media to which you want to enable jobs, click **View** and then click **Media**.
2. From the Media List dialog box, right-click on the media for which you wish to enable jobs and select **Allow Copy**.
   - To select multiple media items, hold down the **Ctrl** key, and right click on the media.
3. Click **Yes** on the Confirmation pop-up window.

ENABLE/DISABLE STREAM RANDOMIZATION

Required Capability: See Capabilities and Permitted Actions

To enable stream randomization:

1. From the CommCell Browser, right click the storage policy for which you want to enable stream randomization, then click **Properties**.
2. From the General tab of the **Storage Policy Properties** dialog box, mark the checkbox for **Enable Stream Randomization**. Note that this field is only enabled when the storage policy is configured to use more than one (1) data stream.
3. Click **OK**.

   To disable this feature, deselect the checkbox.

TUNE STREAM RANDOMIZATION

Required Capability: See Capabilities and Permitted Actions

To tune the stream randomization feature:

1. From the **Control Panel**, double-click **Media Management**.
2. From the **Resource Manager Configuration** tab of the **Media management Configuration** dialog box, perform the following:
   - In the **Interval (in minutes) to calculate valid data size for streams** field specify the interval to calculate the data size for streams.
   - In the **Threshold (in GB) to decide how to distribute data among streams for backup** field specify the threshold to decide data distribution among streams.
3. Click **OK** to save the changes.

RE-COPY FULLY OR PARTIALLY COPIED JOBS

Required Capability: See Capabilities and Permitted Actions

To recopy fully or partially copied jobs:

1. From the right pane of the CommCell Browser, right-click the storage policy copy whose data protection operations you want to recopy, click **View** and then click **Jobs**.
2. Select the necessary filter options in the Job Filter for Storage Policy Copy dialog box.
3. Click the **Advanced** button for additional filter options in the Jobs in Storage Policy Advanced Filter Options dialog box.
4. Click **OK**.
5. A list of jobs associated with a storage policy copy is displayed in the Jobs for Storage Policy Copy window.
6. Right click on a job to be recopied and select **Re-Copy** from the popup menu.

NOTES

- Data can only be recopied if it still exists in the source copy.

RE-COPY ALL JOBS ASSOCIATED WITH A MEDIA

Required Capability: See Capabilities and Permitted Actions

To re-copy all jobs associated with a media:

1. From the right pane of the CommCell Browser, right-click the copy whose media you want to disable, click **View** and then click **Media**.
2. From the Media List dialog box, right-click on the media for which you wish to recopy jobs and select **Re-Copy**.
3. Click **Yes** on the Confirmation pop-up window.

RECOVER YOUR DATA FROM COPIES

Required Capability: See Capabilities and Permitted Actions

To browse/restore/recover data from a specific synchronous or selective copy:

1. Identify the storage policy that will be accessed by the data recovery operation.
2. Identify the copy precedence number for each copy type of your storage policy using the Copy Precedence tab of the **Storage Policy Properties** dialog box.
3. From the Advanced Browse Options dialog box, select the **Browse from copy precedence** option and then type or specify the precedence number in **Copy Precedence**.
4. Data will be restored/recovered from the storage policy copy that has the selected copy precedence.

RESTORE DATA FROM A SECONDARY COPY USING A THIRD-PARTY COMMAND LINE

Related Topics

- Third-Party Command Line Operations

Restore the Oracle Database and Control File from a Secondary Copy using the RMAN Command Line

Before You Begin

- Ensure that you have run a backup of the Oracle database with one or more streams and, if applicable, the control file.
- Ensure that you have run an auxiliary copy operation after completing the backup(s).

Required Capability: See Capabilities and Permitted Actions

To restore the Oracle database and control file from a secondary copy using the RMAN command line:

1. If applicable, restore the control file from autobackup using a secondary copy (otherwise skip to Step 2). To do this, run the script below from the RMAN command line:

   ```
   run {

   allocate channel ch1 type 'sbt_tape'

   PARMS="ENV=(CV_restCopyPrec=1)" TRACE 0;

   allocate channel ch2 type 'sbt_tape'

   PARMS="ENV=(CV_restCopyPrec=2)" TRACE 0;

   restore controlfile from autobackup ;

   }
   ```

2. Run the script below from the RMAN command line to restore the Oracle database from a secondary copy:

   ```
   run {

   allocate channel ch1 type 'sbt_tape'

   PARMS="ENV=(CV_restCopyPrec=1)" TRACE 0;

   allocate channel ch2 type 'sbt_tape'

   PARMS="ENV=(CV_restCopyPrec=2)" TRACE 0;

   restore database;

   }
   ```

Restore the SAP Database from a Secondary Copy using the SAP Command Line

Before You Begin

- Ensure that you have run a backup of the SAP database.
- Ensure that you have run an auxiliary copy operation after completing the backup.

Required Capability: See Capabilities and Permitted Actions

To restore the SAP database from a secondary copy using the SAP command line:

1. Edit the parameter file for the SAP for Oracle *i*DataAgent or SAP for MAXDB *i*DataAgent to include the following two parameter lines:

   ```
   CV_restCopyPrec

   2
   ```

   - For SAP for Oracle on Unix, include the above lines in the `initCER.utl` file located under the `dbs` directory.
   - For SAP for Oracle on Windows, create a parameter file to include the above lines then execute **`brrestore`** with option **`-r`**.

- For SAP for MAXDB on Unix, include the above lines in the parameter file located under the `$<software install folder>\SapMaxDbAgent` directory.
- For SAP for MAXDB on Windows, include the above lines in the parameter file located in the same directory as `BSI_ENV`. To determine the directory where `BSI_ENV` resides, open the `test1.cfg` file located in the install directory then find the PATH for `BSI_ENV` (for example: `D:\MaxDB\sdb\test1\files\backint.conf`).

2. After editing the parameter file as described in Step 1, execute a restore from the SAP command line, and the data will be restored from a secondary copy.

SELECT A SOURCE MEDIAAGENT FOR AN AUXILIARY COPY OPERATION

Required Capability: See Capabilities and Permitted Actions

Do not select a source MediaAgent for this operation unless the source copy is configured with a shared library. If an invalid MediaAgent is selected for the operation, it will fail.

To select a source MediaAgent for an auxiliary copy operation:

1. From the CommCell Browser, right-click the storage policy for which you want to perform an auxiliary copy, click **All Tasks**, and then click **Run Auxiliary Copy**.
2. Select the **Source MediaAgent** for the auxiliary copy.
3. Continue configuring the auxiliary copy operation as outlined in Start an Auxiliary Copy.

EXPORT MEDIA USING VAULT TRACKER

Required Capability: See Capabilities and Permitted Actions

To export media using Vault Tracker:

1. From the CommCell Browser, right-click the **VaultTracker Policies** icon under the Policies node, and then click **New Tracking Policy**.
2. From the wizard, enter a name and description in the **Policy Name** and **Description** boxes. Click **Next**.
3. Click **Standard** and then click **Next.**
4. Select only the secondary copies whose tapes need to be taken offsite. Click **Next**.
5. Select the library from which you want the media exported. Click **Next**.
6. Select the media status to be managed by the policy. Click **Next**.
7. Select an export location from the **Export** dropdown list. Click **Next**.
8. Click **Yes**, and then click **Next**.
9. Define the Vault Tracker policy schedule to occur either every day or every week depending upon how often you need to take the media offsite. Click **Next**.
10. Select the time of day when you need the tapes to start appearing in the mail slot. Click **Next**.
11. Select the start date, and end date and time. Click **Next**.
12. Confirm your selections for the policy. Click **Finish**.
13. Manually remove media from the mail slot.

SET JOB PRIORITIES TO COPY DURING AUXILIARY COPY OPERATION

1. Logon to CommServe computer.
2. Create a text file with the following name under `<Software_Installation_Directory>\Base` folder.

   <StoragePolicyName>_<CopyName>_Jobs.txt
3. In the text file specify **JobID** and **CommCellID** in the following format:

   Syntax

   ```
   JobID, CommCellID
   ```

   Where

  - ○ JobID - The job id of the jobs for which you are setting up the priority
  - ○ CommCellID - The CommCell ID of the CommServe. The value of this parameter is 2.

    Note that this value is not the same as the CommCell ID value in the **License Administration** dialog box

   For example:

   If `8287, 8288, 8289, 8290` jobs are available on primary copy then specify the jobs in the following format:

```
8288, 2
8290, 2
```

4. Perform the Auxiliary Copy operation on the Storage Policy that is specified in the text file name.
5. Once the Auxiliary Copy operation is run, the jobs specified in the text file (e.g., `8288` and `8290`) will be copied first and then the other jobs will be copied. Jobs may not necessarily be copied in the exact order as in the text file but will be copied before other jobs that are not listed in the text file.

   During this process, if Auxiliary Copy job goes into **Waiting**/**Suspended**/**Pending** state (e.g., if the job is interrupted by Job Manager or suspended by the user), then the priority of the jobs using text file will not be considered when the Auxiliary Copy job is resumed. It will copy all the jobs sequentially to secondary storage.

Back to Top

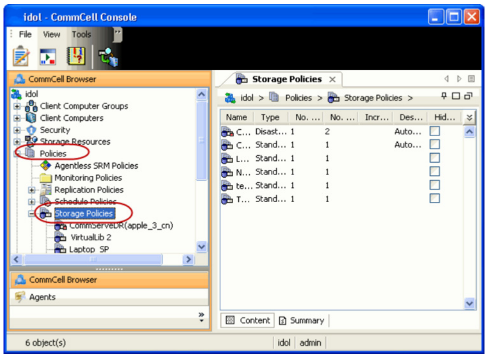
Data Aging - Getting Started

Getting Started	Advanced	Troubleshooting	FAQ	Support

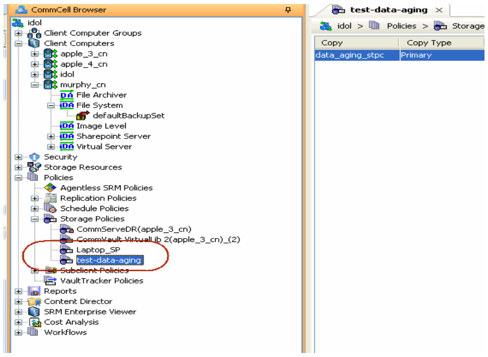
Data Aging is the process of removing old data from secondary storage to allow the associated media to be reused for future backups.

By default, all backup data is retained infinitely. However, you should change the retention of your data based on your needs. Note that if you continue to have infinite retention, you will also need infinite storage capacity.

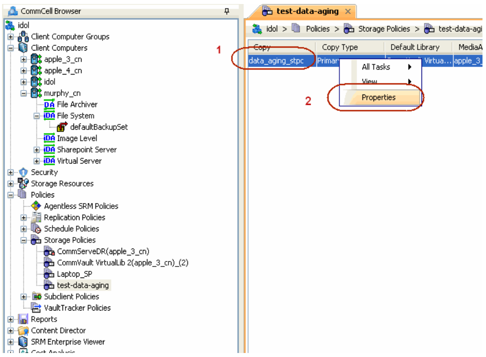
1. From the CommCell Browser, navigate to **Policies | Storage Policies**.



2. Highlight the **Storage Policy**.

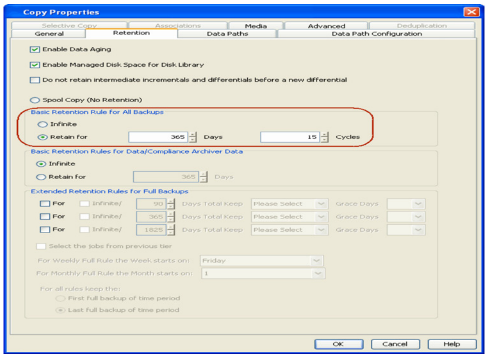


3. From the right pane, right-click the **Storage Policy Copy** and click the **Properties**.



4.

- Click the **Retention** tab.
- Click the **Retain For** in the **Basic Retention Rules for All Backups** area.
- Enter number of days to retain the data.
- Enter number of cycles to retain the data.
- Click **OK**.



☑ Enable Data Aging

☑ Enable Managed Disk Space for Disk Library

□ Do not retain intermediate incrementals and differentials before a new differential

○ Spool Copy (No Retention)

Basic Retention Rule for All Backups

○ Infinite

● Retain for 365 Days 15 Cycles

Basic Retention Rules for Data/Compliance Archiver Data

● Infinite

○ Retain for 365 Days

Extended Retention Rules for Full Backups

□ For □ Infinite/ 90 Days Total Keep Please Select Grace Days

□ For □ Infinite/ 365 Days Total Keep Please Select Grace Days

□ For □ Infinite/ 1825 Days Total Keep Please Select Grace Days

□ Select the jobs from previous tier

For Weekly Full Rule the Week starts on: Friday

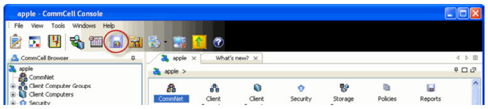
For Monthly Full Rule the Month starts on: 1

For all rules keep the:

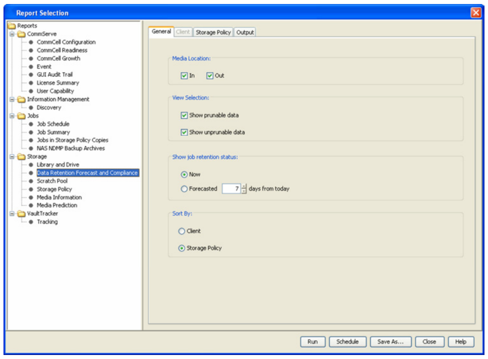
○ First full backup of time period

● Last full backup of time period

5. From the CommCell Browser, click the **Reports** icon.



6. Expand Reports and select **Data Retention Forecast and Compliance.**



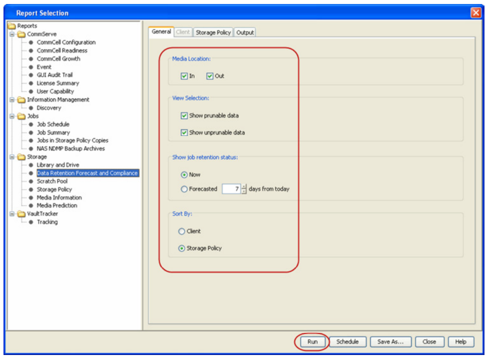
Media Location: ☑ In ☑ Out

View Selection: ☑ Show prunable data ☑ Show unprunable data

Show job retention status: ● Now ○ Forecasted 7 days from today

Sort By: ○ Client ● Storage Policy

7. Click **Run**.



Media Location: ☑ In ☑ Out

View Selection: ☑ Show prunable data ☑ Show unprunable data

Show job retention status: ● Now ○ Forecasted 7 days from today

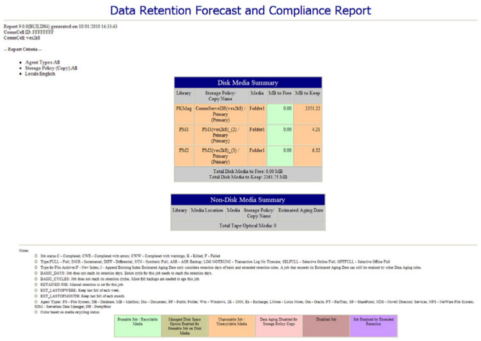
Sort By: ○ Client ● Storage Policy

8. The report will display the data to be pruned when a data aging job is run.

   To ensure only data intended for aging is actually aged, it is important to identify the data that will be aged based on the retention rules you have configured. Hence, ensure this report includes only the data you intend to age.

   If necessary, fine-tune your rules so that only the intended data is aged.

   Once you run a data aging job, the data will be lost.



Data Retention Forecast and Compliance Report

Report 9.0.0(BUILD84) generated on 10/01/2010 14:33:43
CommCell ID: FFFFFFFF
CommCell: vex2k8

-- Report Criteria --

- Agent Types:All
- Storage Policy (Copy):All
- Locale:English

Disk Media Summary				
Library	Storage Policy/ Copy Name	Media	MB to Free	MB to Keep
PKMag	CommServeDR(vex2k8) / Primary (Primary)	Folder1	0.00	2351.22
PM1	PM1(vex2k8)_(2) / Primary (Primary)	Folder1	0.00	4.21
PM2	PM2(vex2k8)_(3) / Primary (Primary)	Folder1	0.00	6.32
Total Disk Media to Free: 0.00 MB Total Disk Media to Keep: 2361.75 MB				

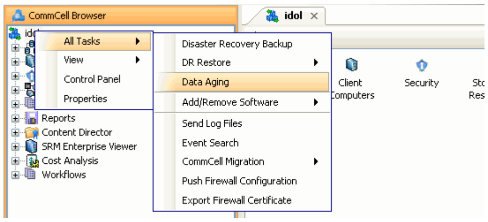
Non-Disk Media Summary				
Library	Media Location	Media	Storage Policy/ Copy Name	Estimated Aging Date
Total Tape/Optical Media: 0				

Notes:

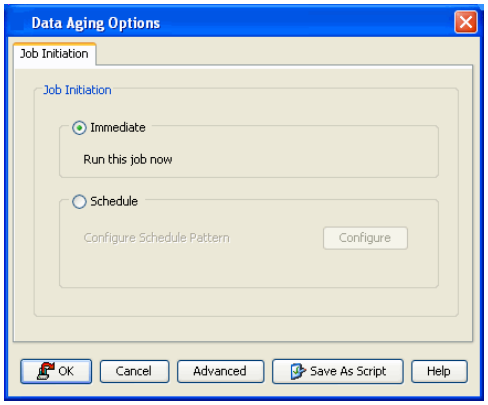
- Job status:C - Completed; CWE - Completed with errors; CWW - Completed with warnings; K - Killed; F - Failed
- Type:FULL - Full; INCR - Incremental; DIFF - Differential; SYN - Synthetic Full; ASR - ASR Backup; LOG NOTRUNC - Transaction Log No Truncate; SELFULL - Selective Online Full; OFFFULL - Selective Offline Full
- Type for File Archiver:F - New Index; I - Append Existing Index Estimated Aging Date only considers retention days of basic and extended retention rules. A job that exceeds its Estimated Aging Date can still be retained by other Data Aging rules.
- BASIC_DAYS: Job does not reach its retention days. Entire cycle for this job needs to reach the retention days.
- BASIC_CYCLES: Job does not reach its retention cycles. More full backups are needed to age this job.
- RETAINED JOB: Manual retention is set for this job.
- EXT_LASTOFWEEK: Keep last full of each week.
- EXT_LASTOFMONTH: Keep last full of each month.
- Agent Types: FS - File System; DB - Database; MB - Mailbox; Doc - Document; PF - Public Folder; Win - Windows; 2K - 2000; Ex - Exchange; LNotes - Lotus Notes; Ora - Oracle; FT - FasTrax; SP - SharePoint; NDS - Novell Directory Services; NFS - NetWare File System; SDM - Serverless Data Manager; PH - ProxyHost
- Color based on media recycling status:

Prunable Job / Recyclable Media	Managed Disk Space Option Enabled for Prunable Job on Disk Media	Unprunable Job / Unrecyclable Media	Data Aging Disabled for Storage Policy Copy	Disabled Job	Job Retained by Extended Retention

9. From the CommCell Console, right click the CommServe icon and click **All Tasks** | **Data Aging**.



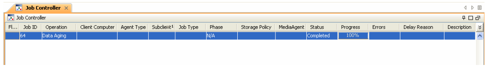
10. Select **Immediate** in the Job Initiation section and click **OK**.



● Immediate
Run this job now

○ Schedule

11. You can track the progress of the job from the **Job Controller** window. When the job has completed, the Job Controller displays **Completed**.



Fl...	Job ID	Operation	Client Computer	Agent Type	Subclient	Job Type	Phase	Storage Policy	MediaAgent	Status	Progress	Errors	Delay Reason	Description
	64	Data Aging					N/A			Completed	100%			

Make sure that the job completes successfully. If the job did not complete successfully, re-run the job.

Data Compression

Topics | How To | Support | Related Topics

OVERVIEW

Data compression options are provided for data secured by data protection operations. Compression reduces the quantity of data sent to storage, often doubling the effective capacity of the media (depending on the nature of the data). If the data is later restored/recovered, the system automatically decompresses the data and restores it to its original state.

The following data compression options are provided:

- Software compression which includes options to compress the data in the:
  - Client
  - MediaAgent
- Hardware compression for libraries with tape media at the individual data path

As compressed data often increases in size if it is again subjected to compression, the system only applies one type of compression for a given data protection operation. You can redefine the compression type at any time without compromising your ability to restore/recover data.

When hardware compression is available and applied, it has precedence over the other compression selections. If hardware compression is enabled for a data path, then all data conducted through that data path is compressed using the hardware compression. If hardware compression is disabled for a data path, then the data is handled in accordance with the software compression selection of each subclient that backs up to the data path. Selections under each subclient include options for Client compression, MediaAgent compression, or no compression.

Also keep in mind that hardware compression is not applicable for disk libraries and hence the software compression selection for subclient is used for data paths associated with disk libraries.

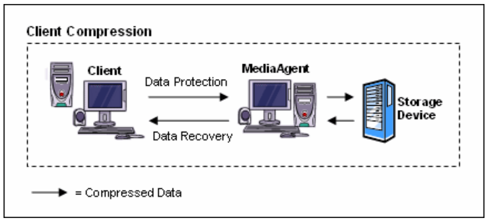
Note that at any given time you can view the compression scheme used for protecting a subclient's data by viewing the details of the data paths associated with the subclient. See View Data Paths Associated With a Subclient for step-by-step instructions.

SOFTWARE COMPRESSION

CLIENT COMPRESSION

The client compression is specified on the subclient level for most agents. (For database *i*DataAgents, this is specified on the instance level.)

Client compression is available for all storage media. This scheme compresses the data on the client computer using the compression software. The compressed data is then sent to the MediaAgent which in turn directs it to a storage media. Client compression is useful if the client and MediaAgent reside on separate computers and therefore the client must send its data using a network. Client compression reduces the network load since the data is compressed before it leaves the client.



Note that client compression may not be suitable in all circumstances. Using software to compress data can be processor intensive. Consequently, you may not want to use client compression for client systems with limited processing power. In such cases, MediaAgent compression may be more efficient.

The diagram on the right illustrates Client Compression.

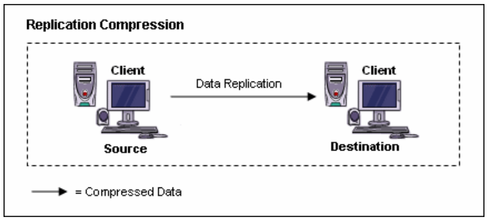
CONSIDERATIONS FOR QUICK RECOVERY AGENT

For the Quick Recovery Agent, when the client compression is enabled, objects are compressed on the source computer in the beginning of the copy and uncompressed on the destination computer at the end of the copy.

REPLICATION COMPRESSION

Data being replicated can be compressed between the source and destination computers. When compression is enabled, data is compressed on the source computer, replicated across the network to the destination computer, and uncompressed on the destination computer, thereby reducing the network load. Compression for replication is specified on the Replication Set level, and applies to all of its Replication Pairs. For a given Replication Set, you can enable or disable client compression between the source and destination machines. See Enable or Disable Software Compression for a Replication Set for step-by-step configuration instructions.

The diagram on the right illustrates Replication Compression.

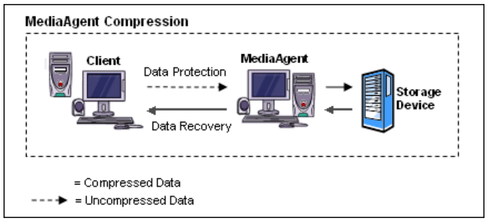


MEDIAAGENT COMPRESSION

The MediaAgent compression is specified on the subclient level for most agents. (For database *i*DataAgents like SAP for Oracle, Oracle, etc. the compression type is specified on the instance level). For a given subclient or instance as appropriate, you can enable or disable MediaAgent compression for all data paths which do not have hardware compression enabled.

MediaAgent compression is available for all storage media. This scheme compresses the data on the MediaAgent using compression software in the MediaAgent. The compressed data is then sent from the MediaAgent to the storage media. MediaAgent compression can be useful if the MediaAgent software resides on a computer that is more powerful than the client computer. Using software to compress data can be processor intensive; consequently, you may want to use MediaAgent compression for client computers with limited processing power.

The diagram on the right illustrates MediaAgent Compression.



Note that data compressed on the MediaAgent during data protection, is decompressed on the client computer during the data recovery.

See the following procedures for step-by-step instructions on enabling (or disabling) software compression:

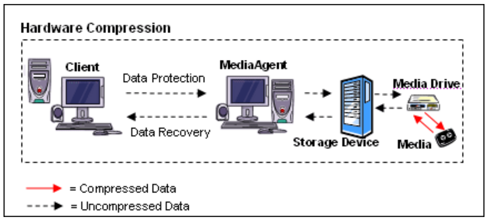
- Enable or Disable Software Compression for a Subclient
- Enable or Disable Software Compression and Network Bandwidth for a QR Subclient
- Enable or Disable Software Compression for Command Line Backups (DB2, Informix, Oracle, Oracle RAC, SAP for Oracle, SAP for MAXDB)
- Enable or Disable Software Compression for Log Backups (DB2, Informix, Oracle, Oracle RAC, Sybase)
- Enable or Disable Software Compression for Oracle Archive Log Backups (Oracle)
- Enable or Disable Software Compression for Oracle Command Line Backups (Oracle)
- Enable or Disable Software Compression for a Replication Set

HARDWARE COMPRESSION

The hardware compression is established on the data path level. This kind of compression is only available for data paths that direct data to tape libraries. This compression scheme sends uncompressed data from the client computer through the data path to the media. There the tape drive hardware compresses the data before writing it to the media.

Generally, hardware compression is faster than software compression since it is performed by dedicated circuitry. This compression scheme is particularly suited for direct-connect configurations where the subclient and MediaAgent are hosted by the same physical computer. In such configurations, there are no network bottlenecks that can throttle the transfer of data to the media drives. Therefore, the drives can compress the data as quickly as it is sent by the subclient. In such configurations, hardware compression can not only boost the virtual capacity of the tape but the performance of the data protection operation as well, because the tape, operating at high speed, stores more data per unit time than it would otherwise.

The diagram on the right illustrates Hardware Compression.



Note that hardware compression is only supported by tape libraries. Hardware compression is not applicable for disk and optical libraries.

Hardware compression may be less useful when data secured by data protection operations must compete with other data for network bandwidth. If the network becomes congested, the tape drives can become starved for data. In this condition, the drives still compress the data, but because data is not supplied quickly enough, the drives must stop and restart the media as more data becomes available. As a result, performance may suffer.

See Enable or Disable Hardware Compression for step-by-step instructions.

NAS *i*DATAAGENTS

Note the following for using Hardware Data Compression for data protection operations involving the NAS *i*DataAgents:

- For a tape drive attached to a NetApp file server, hardware compression is always on.
- For a tape drive attached to a BlueArc or EMC Celerra file server, hardware compression can be configured in the normal manner.
- For any of the NAS *i*DataAgents, when using NDMP Remote Server (NRS) and a drive pool configured to a MediaAgent, hardware compression can be configured in the normal manner.

IMPORTANT CONSIDERATIONS

- ### DEDUPLICATION AND DATA COMPRESSION

  When deduplication storage policy is configured, compression is automatically enabled on the storage policy copy. All subclients associated to the deduplication storage policy will use the compression settings set on the storage policy copy. When the subclient is associated to deduplicated storage policy, by default **Use Storage Policy Settings** option is enabled at subclient level.

  For non-deduplicated storage policy, the compression settings need to be configured on the subclient level and depending upon your environment select On Client or On MediaAgent compression options.

- ### AUXILIARY COPY AND DATA COMPRESSION

  Software compressed data is not uncompressed during an auxiliary copy operation.

- ### NETWARE FILE SYSTEM *I*DATAAGENT

  The NetWare File System data can be in compressed format on a volume that supports compression, and data in compressed format can only be restored to a volume that supports compression. The **Decompress Data before Backup** option allows you to select whether to decompress data that is in compressed format on the backup media and can be restored to either a compressed or uncompressed volume. By default, data is backed up in a compressed format if the data is on a volume that supports compression.

  See Enable Decompress Data before Backup for a NetWare File System Backup Set for step by step instructions.

- ### SUBCLIENT POLICIES AND SOFTWARE COMPRESSION

  Software Compression is made part of subclient policy. Once the subclient policy is associated to a backup set, software compression can be overridden at subclient, if necessary.

- ### DATA SCAN METHOD AND DATA COMPRESSION ISSUE

  While configuring the Windows File System backup sets, if you are using **Data Classification** as the scan method, you may face the following data compression issue: When the data is restored, a non-compressed file, in a compressed folder, becomes compressed. This issue does not occur if you use the **Change Journal** or **Classic Scan** as the scan method during the backup.

Back to Top

Data Compression - How To

Topics | How To | Support | Related Topics

Software Compression

Enable or Disable Software Compression for a Subclient

Enable or Disable Software Compression and Network Bandwidth for a QR Subclient

Enable or Disable Software Compression for Command Line Backups (DB2, DB2 DPF, Informix, Oracle, Oracle RAC, SAP for Oracle, SAP for MAXDB)

Enable or Disable Software Compression for Log Backups (DB2, DB2 DPF, Informix, Oracle, Oracle RAC, Sybase)

Enable or Disable Software Compression for Oracle Archive Log Backups (Oracle)

Enable or Disable Software Compression for Oracle Command Line Backups (Oracle)

Enable or Disable Software Compression for a Replication Set (ContinuousDataReplicator)

Hardware Compression

Enable or Disable Hardware Compression

Replication Compression

Configure Software Compression for a Replication Set

General

Enable Decompress Data before Backup for a NetWare File System Backup Set

View Data Paths Associated With a Subclient

ENABLE OR DISABLE SOFTWARE COMPRESSION FOR A SUBCLIENT

Before you Begin

- Do not enable/disable software compression for a subclient that is being backed up/archived.

Required Capability: Capabilities and Permitted Actions

➧ To enable software compression for a subclient:

1. From the CommCell Browser, right-click the subclient for which you wish to enable software compression and then click **Properties**.
2. Click the **Storage Device** tab and from the Data Storage Policy tab, select the storage policy from the **Storage Policy** list.

   If applicable for the selected agent, click the Log Storage Policy tab and select a storage policy from the **Transaction Log Storage Policy** list.
3. Click the Storage Device (Data Transfer Option) tab and choose the appropriate compression option for this subclient.
   - **On Client** to enable compression on the client computer.
   - **On MediaAgent** to enable compression on the MediaAgent computer.
   - **Use Storage Policy Settings** to use the settings enabled on the deduplication storage policy copy.

     When this option is enabled on the subclient, the backup jobs currently running for this subclient will not reflect the compression settings on the **Job Details** dialog box, that is the **Software Compression** field in the **Backup Job Details** dialog box of the running job displays as **Off** even though the backup job uses compression. You can ignore this and continue running the jobs.

     The status of **Software Compression** field is displayed correctly after completion of a job.
   - **Off** to disable the compression.
4. Click **OK** to save your changes.

This task is now complete.

ENABLE OR DISABLE SOFTWARE COMPRESSION AND NETWORK BANDWIDTH FOR A QR SUBCLIENT

Before you Begin

- Do not change the software compression while a QR Volume Creation operation is running on the subclient.

Required Capability: Capabilities and Permitted Actions

➧ To enable software compression and Network Bandwidth for a QR subclient:

1. From the CommCell Browser, right-click the subclient of a QR Agent for which you wish to enable software compression, then click **Properties** from the shortcut menu.
2. Click the General tab of the Subclient Properties dialog box.
3. Select the **Compression ON** option to enable software compression.
4. Click the **Throttle Network Bandwidth (MB/HR)** option and then enter the throughput as needed.
5. Click **OK** to save your changes.

This task is now complete.

Enable or Disable Software Compression for Command Line Backups

Before you Begin

- Do not enable/disable software compression for an instance or subclient that is being backed up.

Required Capability: Capabilities and Permitted Actions

To enable or disable software compression for Command Line Backups:

1. From the CommCell Browser, right-click the instance you want to modify, and then click **Properties** from the short-cut menu.
2. To enable or disable software compression for command line backups, click the **Storage Device** Data Transfer Option tab and select the appropriate option.
3. Click **OK** to save the changes.

This task is now complete.

Enable or Disable Software Compression for Log Backups

Before you Begin

- Do not enable/disable software compression for an instance or subclient that is being backed up.

Required Capability: Capabilities and Permitted Actions

To enable software compression for Log Backups:

1. From the CommCell Browser, right-click a subclient of the instance containing the Log Backups that you wish to enable software compression for, and then click **Properties**.
2. Click the **Storage Device** tab of the **Subclient Properties** dialog box.
3. To enable or disable software compression for Archive Log Backups, click the Data Transfer Option tab and choose the appropriate compression option.

   Note that when you change the compression scheme for logs, you change it for data as well. Similarly, when you change the compression scheme for data, you change it for logs as well.

4. Click **OK** to save your changes.

This task is now complete.

Enable or Disable Software Compression for Oracle Archive Log Backups

Before you Begin

- Do not enable/disable software compression for an instance or subclient that is being backed up.

Required Capability: Capabilities and Permitted Actions

To enable software compression for Oracle Archive Log Backups:

1. From the CommCell Browser, right-click a subclient of the instance containing the Archive Log Backups that you wish to enable software compression for, and then click **Properties**.
2. Click the **Storage Device** tab of the **Subclient Properties** dialog box.
3. To enable or disable software compression for Archive Log Backups, click the Software Compression tab and choose the appropriate compression option.

   Note that when you change the compression scheme for Archive Logs you change it for data as well, and vice versa.

4. Click **OK** to save your changes.

This task is now complete.

Enable or Disable Software Compression for Oracle Command Line Backups

Before you Begin

- Do not enable/disable software compression for an instance or subclient that is being backed up.

Required Capability: Capabilities and Permitted Actions

▶ To enable or disable software compression for Oracle Command Line Backups:

1. From the CommCell Browser, right-click the instance you want to modify, and then click **Properties** from the short-cut menu.
2. To enable or disable software compression for command line backups, click the **Storage Device** Software Compression tab and select the appropriate option.
3. Click **OK** to save the changes.

This task is now complete.

ENABLE OR DISABLE SOFTWARE COMPRESSION FOR A REPLICATION SET

Before you Begin

- Compression settings made at the Replication Set level are for compression of data between the source computer and the destination computer.

Required Capability: Capabilities and Permitted Actions

▶ To enable/disable software compression for a Replication Set:

1. From the CommCell Browser, right-click the Replication Set and select **Properties**.
2. From the Replication Set Properties (Replication Options) tab, either select or clear **Compression ON**.
3. Click **OK** to save your settings and close the Replication Set Properties.

ENABLE OR DISABLE HARDWARE COMPRESSION

Required Capability: See Capabilities and Permitted Actions

▶ To enable or disable hardware compression:

1. Right-click the storage policy copy and then click **Properties**.
2. Click the Data Paths tab.
3. Click the data path for which you wish to change the hardware compression and then click Properties.
4. From the Data Path Properties dialog box, select the **Hardware Compression** checkbox to enable or de-select to disable hardware compression.
5. Click **OK** to save your changes.

ENABLE DECOMPRESS DATA BEFORE BACKUP FOR A NETWARE FILE SYSTEM BACKUP SET

Before You Begin

- Review Decompress Data before Backup

Required Capability: Capabilities and Permitted Actions

▶ To enable Decompress Data before Backup:

1. From the CommCell Browser, right-click the backup set of a NetWare File System *i*DataAgent for which you want to enable decompression, then click **Properties**.
2. In the General tab, select **Decompress Data before Backup**.
3. Click **OK** to save your change.

This task is now complete.

VIEW DATA PATHS ASSOCIATED WITH A SUBCLIENT

Required Capability: See Capabilities and Permitted Actions

▶ To view data paths:

1. From the CommCell Browser, right-click the subclient whose data paths you want to view, then click **Properties** from the shortcut menu.
2. Click the Storage Device tab of the Subclient Properties dialog box.

3. From the **Data [or Logs] Storage Policy** tab, click **Show Data Paths** to view the data paths used by the subclient to access the storage media for data protection operations. Click **Close** to exit the Data Paths dialog box.
4. Click **OK** to exit the Subclient Properties Storage Device tab.

Back To Top

Data Verification

Topics | How To | Troubleshooting | Related Topics

OVERVIEW

The software typically protects/archives data on various types of media. Once these operations have been performed, there is no way to ascertain if the data is valid for recovering until a data recovery operation has been performed on that data.

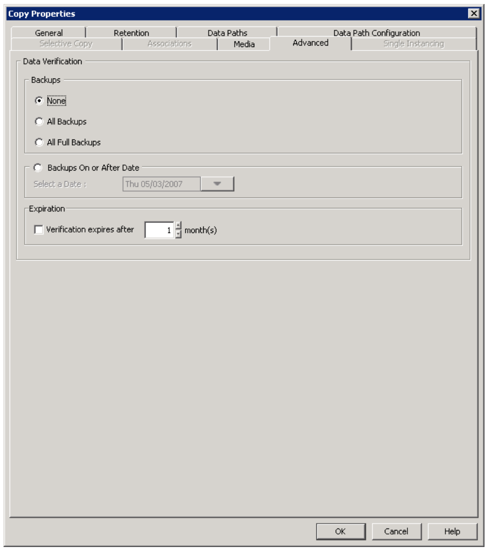
During a data verification operation, data is checked to see that it is valid for recovering and for being successfully copied during an auxiliary copy operation. You can verify data on all copies, or on a specific copy, and in parallel streams. A specific data protection/archive operation can also be verified on a copy. It is also possible to define a time interval of how long data verification for a data protection job is valid for a storage policy copy.

> When auxiliary copy, data verification, and content indexing operations are initiated, they will all utilize the same single auxiliary copy manager process, thus reducing the load resources on the CommServe computer.

CONFIGURE A COPY FOR DATA VERIFICATION

You can configure a copy for data verification so that all, full, or those data protection/archive operations occurring on or after a certain date will be verified during a data verification operation. A copy can be configured for data verification from the `Advanced` tab.

Note that data verification is not set by default for any agents.



Data Verification

Backups

● None

○ All Backups

○ All Full Backups

○ Backups On or After Date

Select a Date : Thu 05/03/2007

Expiration

□ Verification expires after 1 month(s)

PICK A JOB FOR DATA VERIFICATION

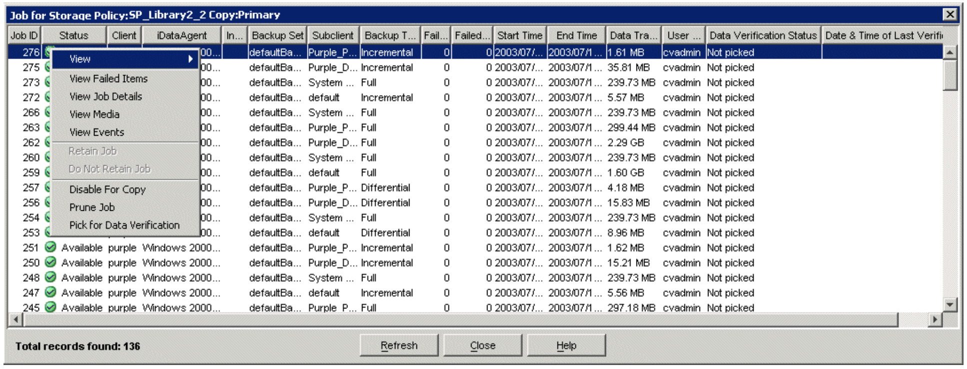
You can select individual jobs to be verified during a data verification operation from the `Jobs for Copy` window. You can verify jobs on all types of storage policies. The example below is for an *i*DataAgent Backup storage policy.

The following table describes the data verification status that is displayed in the `Data Verification Status` column:

Status	When Displayed
`Not Picked`	A job has not been picked for a data verification operation.

Picked for Verification	A job has been picked for a data verification operation.
Successful	A data verification operation ran and successfully verified this job.
Failed	A data verification operation ran and failed to verify this job.
Partial	A data verification operation ran and has not yet completed verifying this job.

Once a job is picked, its status in the Data Verification Status field is displayed as Picked for Verification.

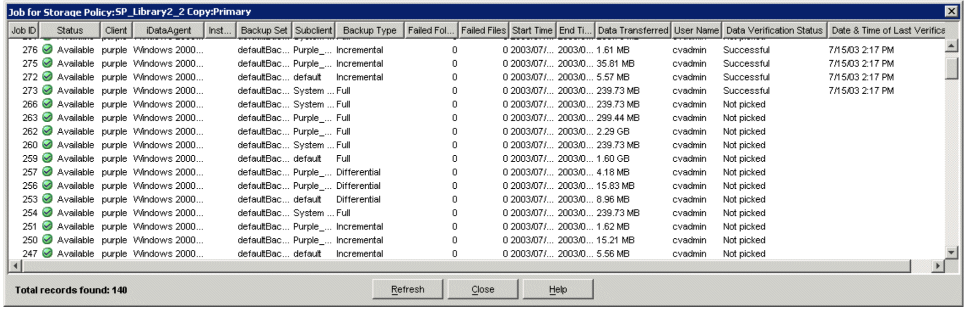


Job for Storage Policy:SP_Library2_2 Copy:Primary

Job ID	Status	Client	iDataAgent	In...	Backup Set	Subclient	Backup T...	Fail...	Failed...	Start Time	End Time	Data Tra...	User ...	Data Verification Status	Date & Time of Last Verifi
276			00...		defaultBa...	Purple_P...	Incremental	0	0	2003/07/...	2003/07/1 ...	1.61 MB	cvadmin	Not picked	
275			00...		defaultBa...	Purple_D...	Incremental	0	0	2003/07/...	2003/07/1 ...	35.81 MB	cvadmin	Not picked	
273			00...		defaultBa...	System ...	Full	0	0	2003/07/...	2003/07/1 ...	239.73 MB	cvadmin	Not picked	
272			00...		defaultBa...	default	Incremental	0	0	2003/07/...	2003/07/1 ...	5.57 MB	cvadmin	Not picked	
266			00...		defaultBa...	System ...	Full	0	0	2003/07/...	2003/07/1 ...	239.73 MB	cvadmin	Not picked	
263			00...		defaultBa...	Purple_P...	Full	0	0	2003/07/...	2003/07/1 ...	299.44 MB	cvadmin	Not picked	
262			00...		defaultBa...	Purple_D...	Full	0	0	2003/07/...	2003/07/1 ...	2.29 GB	cvadmin	Not picked	
260			00...		defaultBa...	System ...	Full	0	0	2003/07/...	2003/07/1 ...	239.73 MB	cvadmin	Not picked	
259			00...		defaultBa...	default	Full	0	0	2003/07/...	2003/07/1 ...	1.60 GB	cvadmin	Not picked	
257			00...		defaultBa...	Purple_P...	Differential	0	0	2003/07/...	2003/07/1 ...	4.18 MB	cvadmin	Not picked	
256			00...		defaultBa...	Purple_D...	Differential	0	0	2003/07/...	2003/07/1 ...	15.83 MB	cvadmin	Not picked	
254			00...		defaultBa...	System ...	Full	0	0	2003/07/...	2003/07/1 ...	239.73 MB	cvadmin	Not picked	
253			00...		defaultBa...	default	Differential	0	0	2003/07/...	2003/07/1 ...	8.96 MB	cvadmin	Not picked	
251	✓ Available	purple	Windows 2000...		defaultBa...	Purple_P...	Incremental	0	0	2003/07/...	2003/07/1 ...	1.62 MB	cvadmin	Not picked	
250	✓ Available	purple	Windows 2000...		defaultBa...	Purple_D...	Incremental	0	0	2003/07/...	2003/07/1 ...	15.21 MB	cvadmin	Not picked	
248	✓ Available	purple	Windows 2000...		defaultBa...	System ...	Full	0	0	2003/07/...	2003/07/1 ...	239.73 MB	cvadmin	Not picked	
247	✓ Available	purple	Windows 2000...		defaultBa...	default	Incremental	0	0	2003/07/...	2003/07/1 ...	5.56 MB	cvadmin	Not picked	
245	✓ Available	purple	Windows 2000...		defaultBa...	Purple_P...	Full	0	0	2003/07/...	2003/07/1 ...	297.18 MB	cvadmin	Not picked	

Total records found: 136

Once a data verification operation is run, the date and time of the operation is displayed in the Date and Time of Last Verification column.



Job for Storage Policy:SP_Library2_2 Copy:Primary

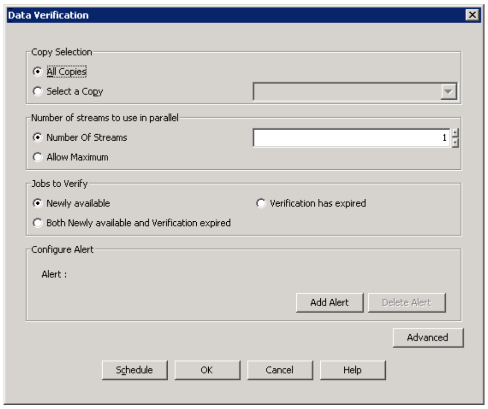
Job ID	Status	Client	iDataAgent	Inst...	Backup Set	Subclient	Backup Type	Failed Fol...	Failed Files	Start Time	End Ti...	Data Transferred	User Name	Data Verification Status	Date & Time of Last Verifica
276	✓ Available	purple	Windows 2000...		defaultBac...	Purple_...	Incremental	0	0	2003/07/...	2003/0...	1.61 MB	cvadmin	Successful	7/15/03 2:17 PM
275	✓ Available	purple	Windows 2000...		defaultBac...	Purple_...	Incremental	0	0	2003/07/...	2003/0...	35.81 MB	cvadmin	Successful	7/15/03 2:17 PM
272	✓ Available	purple	Windows 2000...		defaultBac...	default	Incremental	0	0	2003/07/...	2003/0...	5.57 MB	cvadmin	Successful	7/15/03 2:17 PM
273	✓ Available	purple	Windows 2000...		defaultBac...	System ...	Full	0	0	2003/07/...	2003/0...	239.73 MB	cvadmin	Successful	7/15/03 2:17 PM
266	✓ Available	purple	Windows 2000...		defaultBac...	System ...	Full	0	0	2003/07/...	2003/0...	239.73 MB	cvadmin	Not picked	
263	✓ Available	purple	Windows 2000...		defaultBac...	Purple_...	Full	0	0	2003/07/...	2003/0...	299.44 MB	cvadmin	Not picked	
262	✓ Available	purple	Windows 2000...		defaultBac...	Purple_...	Full	0	0	2003/07/...	2003/0...	2.29 GB	cvadmin	Not picked	
260	✓ Available	purple	Windows 2000...		defaultBac...	System ...	Full	0	0	2003/07/...	2003/0...	239.73 MB	cvadmin	Not picked	
259	✓ Available	purple	Windows 2000...		defaultBac...	default	Full	0	0	2003/07/...	2003/0...	1.60 GB	cvadmin	Not picked	
257	✓ Available	purple	Windows 2000...		defaultBac...	Purple_...	Differential	0	0	2003/07/...	2003/0...	4.18 MB	cvadmin	Not picked	
256	✓ Available	purple	Windows 2000...		defaultBac...	Purple_...	Differential	0	0	2003/07/...	2003/0...	15.83 MB	cvadmin	Not picked	
253	✓ Available	purple	Windows 2000...		defaultBac...	default	Differential	0	0	2003/07/...	2003/0...	8.96 MB	cvadmin	Not picked	
254	✓ Available	purple	Windows 2000...		defaultBac...	System ...	Full	0	0	2003/07/...	2003/0...	239.73 MB	cvadmin	Not picked	
251	✓ Available	purple	Windows 2000...		defaultBac...	Purple_...	Incremental	0	0	2003/07/...	2003/0...	1.62 MB	cvadmin	Not picked	
250	✓ Available	purple	Windows 2000...		defaultBac...	Purple_...	Incremental	0	0	2003/07/...	2003/0...	15.21 MB	cvadmin	Not picked	
247	✓ Available	purple	Windows 2000...		defaultBac...	default	Incremental	0	0	2003/07/...	2003/0...	5.56 MB	cvadmin	Not picked	

Total records found: 140

If this copy has already been configured for data verification, then individual backups do not have to be selected on the copy.

Perform a Data Verification Operation

The operation can then be performed from the Data Verification dialog box.



Data Verification

Copy Selection

● All Copies

○ Select a Copy

Number of streams to use in parallel

● Number Of Streams: 1

○ Allow Maximum

Jobs to Verify

● Newly available

○ Verification has expired

○ Both Newly available and Verification expired

Configure Alert

Alert :

More advanced options are available from the Advanced Options for Data Verification dialog box, in which you can identify the media in which data should be verified.

Data Verification Considerations for NetApp NAS Client

In addition to verifying data which has been backed up using NRS, data which has been backed up to a library attached to a NetApp file server can also be verified to ensure that it is valid for recovery.

Three Windows registry keys are provided which allow you to redirect NetApp NAS NDMP data verification operations:

- sSaveFileHistory: If turned on, all files in the backup will be written to the AuxCopy log as they are encountered in the backup image.

  Note that this can be a large amount of data. If you choose to turn this option on, it is recommended you increase the log file size.
- sVerifyHeaderOnly: If turned on, the data verification operation will not run through the entire backup image. Instead, it will only process the dump header of the backup.
- sDATAVERIFICATION_DESTINATIONDIR: If turned on, data verification can be performed for Read-Only volumes when a writable location is specified on the file server. This is useful if backing up a Snap mirror destination volume to a tape drive on the file server.

For more information on these registry keys, see Registry Keys and Parameters.

LICENSE REQUIREMENT

This feature requires a Feature License to be available in the CommServe® Server.

Review general license requirements included in License Administration. Also, View All Licenses provides step-by-step instructions on how to view the license information.

AUDIT TRAIL

Operations performed with this feature are recorded in the Audit Trail. See Audit Trail for more information.

RELATED REPORTS

ADMINISTRATIVE JOB SUMMARY REPORT

The Administrative Job Summary Report displays a summary of all or select Administrative jobs.

DATA VERIFICATION JOB SUMMARY REPORT

The Data Verification Job Summary Report displays all data verification jobs with a specified status during a specified time period.

Back to Top

Data Verification - How To

Topics | How To | Troubleshooting | Related Topics

CONFIGURING A STORAGE POLICY COPY FOR DATA VERIFICATION

Required Capability: Capabilities and Permitted Actions

➧ To configure a storage policy copy for data verification:

1. From the right pane of the CommCell Browser, right-click the storage policy, and then click **Properties**.
2. From the Copy Properties (Advanced) tab of the **Copy Properties** dialog box, click the **All Backups** option if you want all backups to be verified during a data verification operation, or click **All Full Backups** if you want only full backups to be verified. You can also click the **Backups On or After Date** option and select a date from the **Select a Date** list. Only those backups that occur on or after the date you select will be verified.

   Additionally, you can select the **Verification Expires after** option and choose the appropriate number of months from the list.
3. Click **OK** to save the changes.

PICK A JOB ON A STORAGE POLICY COPY FOR DATA VERIFICATION

Required Capability: See Capabilities and Permitted Actions

➧ To select a job for data verification:

1. From the right pane of the CommCell Browser, select a storage policy, then right click the storage policy copy whose job(s) you want to pick for data verification, click **View** and then click **Jobs**.
2. Filter the necessary options in the Job Filter for Storage Policy Copy dialog box. Click **OK**.

3. From the Jobs for Storage Policy Copy window, right-click a job, then click **Pick for Data Verification**. If you then decide that you do not want this job to be verified during a data verification operation, right-click the backup and click **Do Not Verify Data**.
4. Click **Close**.

Schedule a Data Verification Operation

Required Capability: Capabilities and Permitted Actions

To schedule a data verification operation.

1. From the CommCell Browser, right-click the storage policy for which you want to verify the data, click **All Tasks**, and then click **Verify Data**.
2. From the Copy Properties (Advanced) dialog box, select either **All Copies**, or a select copy from the **Select a Copy** list.
3. Select the number of streams to verify in parallel from the **Number of Streams to Copy in Parallel** pane, or select **Allow Maximum**. You may also select **Jobs to Verify** if you wish to select specific jobs to verify, as well as **Configure Alert** if you wish to configure a Data Verification Alert.
4. To select more advanced options, click Advanced. Select the appropriate options from the Advanced Options for Data Verification dialog box. Click **OK**.
5. Click **Schedule**.
6. From the Schedule Details tab, select the necessary scheduling options
7. To view the job summary for the data verification operation that you have scheduled, click the Copy Properties (Advanced) tab.
8. Click **OK** to save the schedule.

Start a Data Verification Operation

Required Capability: Capabilities and Permitted Actions

To start a data verification operation:

1. From the CommCell Browser, right-click the storage policy for which you want to verify the data, click **All Tasks**, and then click **Verify Data**.
2. From the Copy Properties (Advanced) dialog box, select either **All Copies**, or a select copy from the **Select a Copy** list.
3. Select the number of streams to verify in parallel from the **Number of Streams to Copy in Parallel** pane, or select **Allow Maximum**. You may also select **Jobs to Verify** if you wish to select specific jobs to verify, as well as **Configure Alert** if you wish to configure a Data Verification Alert.
4. To select more advanced options, click Advanced. Select the appropriate options from the Advanced Options for Data Verification dialog box. Click **OK**.
5. Click **OK**.

Back to Top

Data Integrity Validation

Topics | How To | Troubleshoot | Related Topics

OVERVIEW

Data Integrity Validation allows you to verify the integrity of the data secured by the data protection operations. Data Integrity Validation can be employed to verify the integrity of the data stored in the media, as well as the data transferred over the network.

DATA INTEGRITY VALIDATION ON MEDIA

Data Integrity Validation on Media checks the data restored from the media for any possible data corruption when the data resided in the media. The MediaAgent generates the integrity validation on data during the backup operation, and this is verified with the Data Integrity Validation generated on the data during the restore operation. Note that this option must be enabled during the backup as well as the restore operations.

DATA INTEGRITY VALIDATION ON NETWORK

To verify the integrity of the data transferred over the network, the Data Integrity Validation generated at the respective clients before the data transfer will be verified with the Data Integrity Validation generated at the MediaAgent after the data transfer is complete, and vice versa. This option can be enabled during backup operations, restore operations, or both.

ENABLING DATA INTEGRITY VALIDATION

Data Integrity Validation is enabled at the MediaAgent. This option is disabled by default. Use the following procedures to enable/disable Data Integrity Validation:

- Enable (or Disable) Data Integrity Validation on Media
- Enable (or Disable) Data Integrity Validation on Network

HANDLING DATA INTEGRITY VALIDATION ERRORS

If the Data Integrity Validation fails, the data protection jobs will be moved to a pending state with the corresponding error code and description mentioned in the Reason for Delay field of the job, displayed in the Job Controller. See Job Errors for more information.

The pending jobs can be handled as follows:

- Restore operations can be configured the operation to skip errors and continue with the restore. See Skip Errors and Continue for more information and step-by-step instructions.
- Backup operations can be retried and handled as configured in the Job Retry Options.

SUPPORT INFORMATION

The This feature is supported on all platforms supported by MediaAgent. See System Requirements - MediaAgent platforms supported by MediaAgent.

Consider the following for mixed mode configurations:

- Data Integrity Validation on Media is supported in mixed mode configuration, where the MediaAgent is used with clients from a previous release.
- For Data Integrity Validation on Network, the MediaAgent and the clients must be maintained in the current release.

RELATED REPORTS

JOBS IN STORAGE POLICY COPIES REPORT

The Jobs in Storage Policy Copies Report provides a list of data protection jobs associated with the storage policy copies based on the selected filter criteria. If the Data Integrity Validation for data is enabled for a job, that information is displayed in the Job ID status.

The Data Integrity Validation status is also displayed in the Jobs for Storage Policy Copy window when you view the Jobs of a Storage Policy Copy.

Back to Top

Data Integrity Validation - How To

Topics | How To | Troubleshoot | Related Topics

ENABLE (OR DISABLE) DATA INTEGRITY VALIDATION ON MEDIA

Required Capability: Capabilities and Permitted Actions

➧ To enable or disable Data Integrity Validation on Media:

1. From the CommCell Browser, click the **MediaAgents** icon. All the MediaAgents available in the CommCell are displayed on the right-pane of the CommCell Browser.
2. Right-click the MediaAgent that you wish to enable or disable Data Integrity Validation, and then click **Properties**.
3. From the General tab of MediaAgent Properties, select **Validation on Media** to enable Data Integrity Validation of data stored in the media.
4. Click **OK** to save the configuration.

ENABLE (OR DISABLE) DATA INTEGRITY VALIDATION ON NETWORK

Required Capability: Capabilities and Permitted Actions

➧ To enable or disable Data Integrity Validation for data transferred on Network:

1. From the CommCell Browser, click the **MediaAgents** icon. All the MediaAgents available in the CommCell are displayed on the right-pane of the CommCell Browser.
2. Right-click the MediaAgent that you wish to enable or disable Data Integrity Validation, and then click **Properties**.
3. From the General tab of MediaAgent Properties, select **Validation on Network** to enable Data Integrity Validation for data transferred over the network.
4. Click **OK** to save the configuration.

Hardware Encryption

Topics | How To | Related Topics

Several tape drives like LTO4 support encryption of data on the tape drive. These tape drives provide the necessary controls to the backup applications to get the encryption capabilities as well as set the encryption properties on the drive. Some of tape libraries also provide key management services. Calypso's Hardware Encryption feature provides key management for those tape libraries which do not support key management by themselves.

Key Management for Hardware Encryption can be enabled in one of the two ways:

1. Calypso Software managing the encryption keys
2. Hardware/Library managing the encryption keys

CALYPSO SOFTWARE MANAGING THE ENCRYPTION KEYS

If the library does not have a license to enable the key management, then you can enable it from the Storage Policy copy level.

Key management includes the ability to generate random encryption keys for stored data and also manage the secure storage of these keys. In addition, it also includes the ability to provide a random encryption key for the tape drive to perform the encryption and decryption of the data. The random key is generated for each chunk in the media so that the strength of the encryption is very high. If all the data in a media is encrypted with the same key, it is susceptible to breakages and thus will have lower strength.

> This random key is generated based on FIPS (Federal Information Processing Standard) standards and the same key is not reused for other backup data.

Hardware encryption must be established for each data path and is only available for data paths that direct data to tape libraries.

For each data protection operation, the software checks the drive to see if encryption is supported. If encryption is supported, the software provides the encryption key, which is in turn stored in the CommServe Database Engine when the chunk is written to the media. The encryption key will be stored after scrambling it with a proprietary encryption.

The encryption key gets deleted when the data for that chunk is pruned.

- Hardware encryption must be enabled only when the drives associated with the data path support encryption. If this option is enabled and the hardware does not support encryption, jobs using the data path will go Pending.
- For Data Recovery and Auxiliary Copy operations using the CommCell Console, the specific key will be automatically provided by the software for each chunk.
- For Data Recovery operations using the Media Explorer, an option to store the encryption key on the media is provided in the data path.

HARDWARE/LIBRARY MANAGING THE ENCRYPTION KEYS

If you have a hardware vendor license applied on the library for key management, and it is enabled, then no additional Calypso license and/or configuration is required. In this scenario, the encryption and key management will be done at the hardware level.

The hardware library generates and stores the encryption keys per media and the hardware drive encrypts the data. Therefore, every backup job written to a specific media will have the same key.

> If you have hardware encryption (Key Management) enabled on the hardware side and you also have hardware encryption option enabled at storage policy level, the job would go pending stating that:
>
> "The hardware does not support hardware encryption and hardware encryption option should be disabled at the storage policy level".
>
> This ensures that the key management must be enabled in one of the two available ways. If both are enabled, the hardware/library managing the encryption keys always takes precedence.

SUPPORT

Hardware encryption is supported by all MediaAgents, if the devices attached to these MediaAgents support encryption. Note that hardware encryption is only supported by tape libraries. Hardware encryption is not applicable for disk and optical libraries.

RELATED REPORTS

JOBS ON STORAGE POLICY COPIES REPORT

The jobs on Storage Policy Copies Report display the information of data encryption jobs with superscript HE (Hardware Encryption) status.

AUXILIARY COPY ENCRYPTION

While hardware encryption is the fastest method of encrypting data, you can also encrypt storage policy copies using auxiliary copy encryption. This capability allows you to select portions of data you wish to encrypt and does not require any specialized media or hardware.

See Auxiliary Copy Encryption for more information.

Hardware Encryption - How To

Topics | How To | Related Topics

ENABLE (OR DISABLE) HARDWARE ENCRYPTION

Required Capability: See Capabilities and Permitted Actions

➤ To enable or disable hardware encryption:

1. Right-click the storage policy copy and then click **Properties**.
2. Click the Data Paths tab.
3. Click the data path for which you wish to enable (or disable) hardware encryption and then click **Properties**.
4. From the Data Path Properties dialog box, select the **Hardware Encryption** option to enable; clear this option to disable.

   If enabled, select either the **Via Media Password** or **No Access** options to enable or disable the option to store the encryption keys on the media.
5. Click **OK** to save your changes.

VaultTracker® Feature

Topics | How To | Troubleshoot | Support | Related Topics

OVERVIEW

The **VaultTracker**® feature license provides the capability to track media movement between two locations. It is also used to export media. The following sections describe the features and capabilities specific to the **VaultTracker** feature.

The VaultTracker Enterprise Feature license provides the capability to track media movement between several locations. In addition to the standard VaultTracker features, it also provides several advanced capabilities. For information on the features and capabilities specific to VaultTracker, see VaultTracker Enterprise Feature.

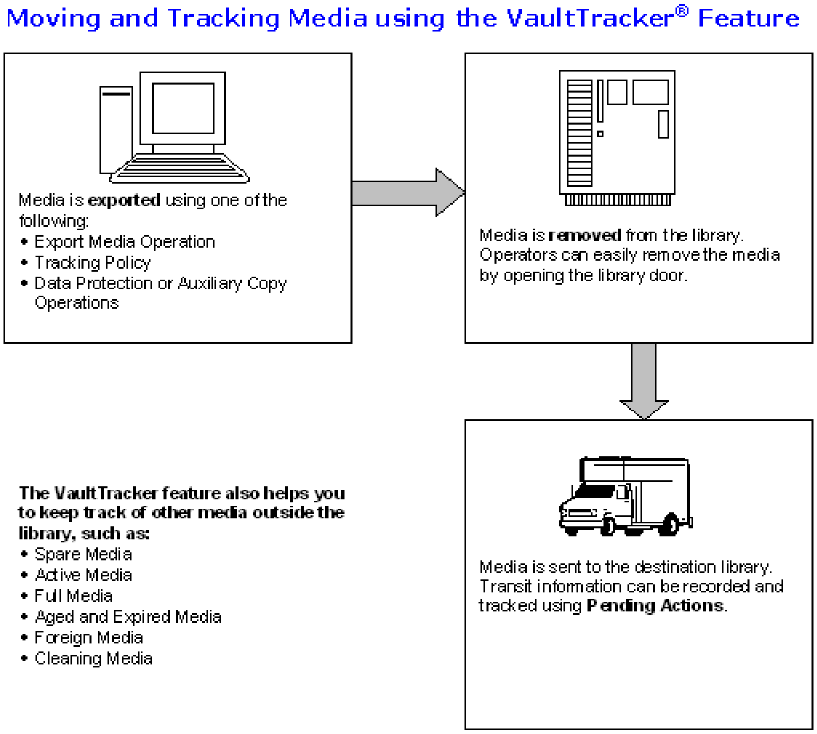
For information on license requirements, see VaultTracker® Licenses in License Administration.

MANAGING MEDIA

The VaultTracker® feature provides the facility to manage media that are removed from a library and stored in offsite locations. In practical terms, the VaultTracker function provides the following capabilities in your day-to-day operations:

- Identifies media that must be sent off-site for storage or brought back from off site locations.
- Automatically moves the media in sequence in the library and provides a pick-up list for the operators.
- Facility to identify and track media during transit.
- Facility to record and track the movement of media not used by all MediaAgents or Foreign Media.

The following diagram provides an overview of the VaultTracker elements:



Moving and Tracking Media using the VaultTracker® Feature

Media is **exported** using one of the following:

- Export Media Operation
- Tracking Policy
- Data Protection or Auxiliary Copy Operations

Media is **removed** from the library. Operators can easily remove the media by opening the library door.

Media is sent to the destination library. Transit information can be recorded and tracked using **Pending Actions**.

The VaultTracker feature also helps you to keep track of other media outside the library, such as:

- Spare Media
- Active Media
- Full Media
- Aged and Expired Media
- Foreign Media
- Cleaning Media

How to Use the VaultTracker® Feature

The following section describes the possible steps involved in tracking media using the VaultTracker capabilities:

1. Initiate the VaultTracker process by exporting the media using the VaultTracker feature.
   - For media that should be exported immediately, you can export the media from a list of available media with VaultTracker features enabled.
   - For media that should be exported once certain criteria are met, you can define one or more Tracking Policies. A standard Tracking Policy can track the movement of media between any source and destination.
2. Once the Export Media operation has been initiated, you can remove the media from the library by ejecting the media from the library's mail-slot. The media can then be easily removed by opening the library door.
3. While the media is in transit, you can track and acknowledge the status of the media using Pending Actions.
   - Use Manual Acknowledgement to track the media manually in the CommCell® Browser.
   - Use Automatic Acknowledgement to automatically acknowledge all pending actions associated with the media as long as the source and destination are locations.
4. View information about the media managed by the VaultTracker feature by generating a Tracking Report, which can include pending actions and media associated with a VaultTracker Policy.

The following sections describe each of these possible steps in depth.

Exporting Media using the VaultTracker® Feature

You can export media using the VaultTracker Feature software and VaultTracker Enterprise Feature in the following ways:

- using the **Export Media Wizard**
- using the **Export Media from a List** feature
- using **VaultTracker Policies**
- after Data Protection and Auxiliary Copy Operations (VaultTracker Enterprise Feature only)

All three methods provide the necessary options to run the export operation immediately or schedule the export operation to run for a later time.

You can configure the number of times an export operation must retry before it is aborted, and the retry interval minutes using the **Export Operation Retry Count** and the **VaultTracker feature export retry interval in minutes** options from the Media Management Configuration (Service Configuration) dialog box available in the **Control Panel**.

The following sections discuss the various export media options in depth.

EXPORTING MEDIA USING THE EXPORT MEDIA WIZARD

The **Export Media Wizard** provides the capability to quickly export one or more media from a library. This wizard is useful if you know the library containing the media you wish to export, as well as the media to be exported. You can choose to export media in 2 ways:

- using the VaultTracker/VaultTracker Enterprise feature, which provides all the options you need create tracking policies.
- from a list of available media in the library, from which you can select the appropriate media to be exported. The media will then be automatically placed in the appropriate mail slot for removal.

The Export Media Wizard is accessible at the **Library** and **Media in Library** levels in the CommCell® Console. See Export Media using the Export Media Wizard for step-by-step instructions.

EXPORTING MEDIA FROM A LIST

Media can be selected from a list of media and exported. This is useful when you wish to export several media at the same time and know either the media's barcode, or slot number in which the media resides. This task can be performed from the following levels in the CommCell® Console:

- **Media List** dialog box which appears when you select the **View Media** option. This dialog box can be accessed by right-clicking a Storage Policy copy.
- **Media List** dialog box which appears when you select the **Change Data Path** option. This dialog box can be accessed by right-clicking a Storage Policy copy.
- **Media List** dialog box which appears when you select the **Media Not Copied** option. This dialog box can be accessed by right-clicking a Storage Policy and Storage Policy copy.

Once the media to be exported is selected, you can choose to use the VaultTracker® feature to track the export operation by clicking on the **Advanced** button in the Export Media List dialog box. A Tracking policy can be created to export media based on the selected criteria.

See Export Media from a List using the VaultTracker Feature for step-by-step instructions.

EXPORTING MEDIA USING TRACKING POLICIES

Tracking Policies help you to define what media must be moved, where it must be moved to, and when it should be moved. This is useful if you wish to schedule routine exports of media that have satisfied certain criteria.

A standard Tracking Policy can be created to track the movement of media between any source and any destination, including:

- Library to location
- Location to location
- Location to library
- Library to library

Once a policy is created, you can view the media associated with that policy by right-clicking on the policy and selecting **View Media**.

When creating a policy, you can:

- Schedule the policy to run at a later time if you anticipate changes being made to the policy prior to media movement taking place. Policies can be scheduled to run daily, weekly, etc., if desired.
- Delay the export of the media, which creates a time gap between when the policy is run and when the media movement actions actually start. This provides time for you to create and review a VaultTracker Report with all the policy's actions detailed prior to any actions taking place. If any changes to the policy are required, you can perform these changes without aborting or rerunning an action.
- Temporarily stop an action by placing the export operation in a pending state for a specified amount of time. This is useful if you need to perform library maintenance or urgent data protection and recovery operations, but do not wish to abort or restart what has already been completed. You can manually restart the policy from the point it left off when the library is available, or you can set the policy to resume automatically at a specific time.

Once created, you can further facilitate Tracking Policies by right-clicking on the policy in the CommCell® Console:

- **Run** the policy if you wish to initiate the policy without further delays or changes to the policy.
- **Clone** the policy to create an exact duplicate of the policy that retains all of the properties of the original policy. Once created, you can edit the properties of the policy, if necessary. This saves you the time of creating a new policy manually. (See Cloning Policies for more information.)

- Change the **Properties** of a policy if you wish to make changes to the configuration of the policy while it is still in the pending state.

For step-by-step instructions on creating and managing tracking policies, see the following:

- Create a Tracking Policy
- Clone a Tracking Policy
- Modify a Tracking Policy
- Delete a Tracking Policy
- View Media Associated with a Tracking Policy
- Run a Tracking Policy
- Schedule a Tracking Policy

See Also: Export Media

REMOVING MEDIA FROM THE LIBRARY

Once the export operation has been initialized, the media can then be removed from the library by ejecting the media from the library mail slots.

RECORDING PENDING ACTIONS

Once media is removed from the library, all media movement outside the library must be recorded to track the operation. Such outside media movements are referred to as **Pending Actions**. Once an action is initiated, the media will be displayed in the reconciliation report.

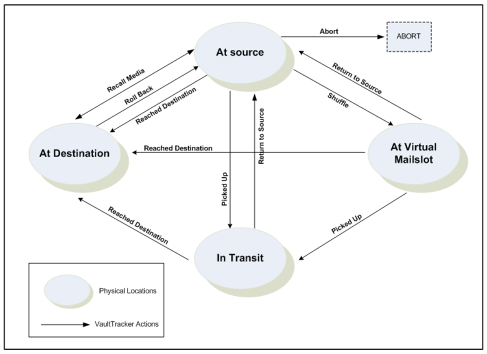
The following list provides links to diagrams that depict the various types of media movements and the options for recording pending actions:

- Media Movement between 2 Locations
- Media Movement from a Library to Location
- Media Movement from a Location to a Library
- Media Movement between 2 Libraries

The following pending actions can be recorded:

- **Picked up** - This option should be used to set the media location as *In Transit*, when the source is a location. (In the case of a library, this option will be automatically performed when the media is removed from the source library.)
- **Reached Destination** - This option should be used to indicate that the media has reached its destination. The pending action is considered to be completed and is displayed in the **Tracking History**. If the final destination is a library, this option will be automatically performed when the media is detected in the destination library.
- **Return to Source** - This option should be used to reset media location to the source location. This option is valid only when:
  - The media is in the in-transit state.
  - When the source is a location. (not a library)
- **Abort** - Aborts the pending action.
- **Suspend** - Temporarily discontinues all media movement for a specified amount of time. The media movement can be resumed manually or at a specified time.
- **Resume** - Media movement continues when a suspension has been lifted by either manually resuming the action or when the specified **Suspend** time has expired.
- **Quit Time** - Specify the amount of time to elapse for the action to abort. This is also configurable in the Media Management Configuration (Service Configuration) dialog box.

The diagram on the right provides a summary of all pending actions. Note that some items are supported for VaultTracker Enterprise only.



You can view the pending actions in the CommCell Browser by right-clicking the **VaultTracker** icon under the **Storage Resources** icon, and then clicking **Actions**. All pending actions are displayed on the right-hand pane.

ACKNOWLEDGING PENDING ACTIONS

The VaultTracker® feature provides two ways of acknowledging pending actions:

- Manual Acknowledgement

- Automatic Acknowledgement

These are explained in the following sections.

MANUAL ACKNOWLEDGMENT

When you run a data protection operation, auxiliary copy operation, Export Media operation, or Tracking Policy with the auto-acknowledge option disabled, you must manually acknowledge the media movement actions. You can record the pending action either for all media associated with a specific movement, or for individual media associated with a specific movement.

There are two methods with which you can manually acknowledge pending actions:

1. **Pre-acknowledge**: All pending actions can be acknowledged assuming that the tapes will get to the destination.
2. **Post-acknowledge**: The Tracking Report with the **Reconciliation** option enabled can be generated. All media which are in transit are listed. Once a confirmation from offsite is received, all Pending Actions can be acknowledged.

See Monitor and Record the Status of a Media for step-by-step instructions.

AUTOMATIC ACKNOWLEDGMENT

When you create a Tracking Policy, you can enable the Auto-Acknowledge option within the policy. When such a policy is run, the system will automatically acknowledge all pending actions associated with the media movement if both source and destination is a location. If the source is a library, the pending actions will be automatically acknowledged when the media is removed from the library.

Note that the automatic acknowledgement option can be enabled (or disabled) for Tracking Policy and Media Export operations. Automatic acknowledgement is not available for Data Protection and Auxiliary copy operations.

See Set Automatic Tracking in a VaultTracker Policy for step-by-step instructions.

VIEWING TRACKING HISTORY

Once all the pending actions are recorded, the VaultTracker® feature automatically catalogs the information in the Tracking History. Tracking History can be viewed from the CommCell® Browser by right-clicking the **Actions** icon under **VaultTracker**, and then clicking **View History**. Filter options for viewing the history are also provided.

If you would like the information to be displayed in the Actions pane before it is moved to the history information, you can establish a display time using the **Time in hours to show the VaultTracker history in actions pane** option from the **Media Management Configuration (Service Configuration)** dialog box available in the **Control Panel**.

See View the Tracking History for step-by-step instructions:

ROLLING BACK AN ACTION

The **Roll Back** option can be performed if both the source and destination locations were export locations and the media is listed in the history information after being marked as reached destination. This option provides the opportunity to rollback a wrong location change.

See Roll Back an Action in the Tracking History for step-by-step instructions.

DELETING AN ACTION

You can **Delete** a pending action history or delete individual media action history of a pending action.

See Delete an Action in the Tracking History for step-by-step instructions.

PRUNING TRACKING HISTORY

Tracking History information is by default pruned after 90 days. If necessary this value can be modified using the **Days to keep VaultTracker® records** option from the **Media Management Configuration (Vault Tracker Configuration)** dialog box available in the **Control Panel**.

LICENSE REQUIREMENTS

For information on license requirements, see VaultTracker® Licenses in License Administration.

RELATED REPORTS

VAULT TRACKING REPORT

The Vault Tracking Report can be generated to view information about media managed by the VaultTracker® feature, including pending actions, spare media that are due back, movement action history, and media related to a VaultTracker policy. Each Vault Tracking Report can be generated and saved in HTML, text, and Iron Mountain Report formats. Optionally, a style sheet can be selected to customize the XML output.

The **Reconciliation** option, if selected, will display all the tapes that are pending their arrival at the destination.

For information on generating and using the Vault Tracking Report, see Vault Tracking Report.

MEDIA INFORMATION REPORT

The Media Information report can be generated by sorting the media based on the export location. This report can then be sent to an offsite person/agency to verify that the contents matches the information in the VaultTracker® records.

Back to Top

VaultTracker Feature - How To

Topics | How To | Troubleshoot | Support | Related Topics

Overview

Track Media using VaultTracker Feature and VaultTracker Enterprise Feature

Tracking Policies

Create a Tracking Policy

Clone a Tracking Policy

Modify a Tracking Policy

Delete a Tracking Policy

View Media Associated with a Tracking Policy

Run a Tracking Policy

Schedule a Tracking Policy

Export Media using VaultTracker

Export Media using the Export Media Wizard

Export Media From a List using VaultTracker

Pending Actions

Set Automatic Tracking in a Tracking Policy

Monitor and Record the Status of a Media

Tracking history

View the Tracking History

Delete an Action in the Tracking History

Roll Back an Action in the Tracking History

Export Locations

Add/Modify a Location

Delete a location

Track Media using VaultTracker Feature and VaultTracker Enterprise Feature

Required Capability: See Capabilities and Permitted Actions

To track media using VaultTracker Feature and VaultTracker Enterprise Feature:

1. Create the list of media that must be tracked. This can be done in one of the following ways:
   - Create a Tracking Policy as described in Create a Tracking Policy.
   - Specify that media associated with a backup job must be exported and tracked as described in Export Media After a Date Protection Operation (VaultTracker Enterprise Feature only), Export Media After An Auxiliary Copy Operation (VaultTracker Enterprise Feature only), and Export Media from a List using VaultTracker.
2. If you have created a Tracking Policy, you must run or schedule the policy, as described in Run a Tracking Policy and Schedule a Tracking Policy.

   If necessary, you can you can view the media associated with a Tracking Policy as described in View Media Associated with a Tracking Policy.
3. Once the media movement is initiated, you must monitor and record the status of the media, as described in Monitor and Record the Status of a Media.
4. Once the media movement is completed, you can view the history information for the media, as described in View Tracking History.

Create a Tracking Policy

Required Capability: See Capabilities and Permitted Actions

To create a Tracking Policy:

1. From the CommCell Browser, right-click the **VaultTracker Policies** icon under the Policies node, and then click **New Tracking Policy**.
2. The **VaultTracker Policy** wizard guides you through the process of creating a new Tracking Policy.

- A regular Tracking policy can be created to export media based on the selected criteria.
- A due back Tracking policy can be created to track the movement of spare media, residing outside the library.
- Once created the Tracking Policy must be run or scheduled, as described in Run a Tracking Policy and Schedule a Tracking Policy.

Clone a Tracking Policy

Required Capability: See Capabilities and Permitted Actions

To clone a tracking policy:

1. From the CommCell Browser, click the **VaultTracker Policies** icon under the **Policies** node.

   All the available Tracking Policies are displayed in the right pane of the CommCell Browser.
2. Right-click the policy that you wish to clone and then click **Clone**.
3. Type the name of the new policy in the **Enter Name box** of the **Clone VaultTracker Policy** dialog box. Click **OK**. The cloned Tracking Policy is displayed in the VaultTracker Policies level of the CommCell Browser.
4. Right-click the Tracking policy, and then click **Properties**. The **Tracking Policy Details** dialog box is displayed.
5. From the **General** tab, click the **Enable** check box. Click **OK**. The Tracking policy is now enabled and ready for use.

- You must enable a cloned Tracking policy after it is created.
- It is recommended that some of the options of the cloned Tracking policy is changed to avoid an exact duplication of the policy.

Modify a Tracking Policy

Required Capability: See Capabilities and Permitted Actions

To modify a tracking policy:

1. From the CommCell Browser, right-click the **VaultTracker Policies** icon under the **Policies** node.

All available Tracking Policies are displayed in the right pane of the CommCell Browser.

2. Right-click the policy that you wish to modify and then click **Properties**.
3. Make the necessary changes in the **Tracking Policy Details** dialog box and then click **OK** to save the information.

DELETE A TRACKING POLICY

Before You Begin

- Ensure that no pending actions are in progress for the tracking policy you wish to delete.

Required Capability: See Capabilities and Permitted Actions

To delete a tracking policy:

1. From the CommCell Browser, right-click the **VaultTracker Policies** icon under the **Policies** node.

   All the available Tracking Policies are displayed in the right pane of the CommCell Browser.
2. Right-click the policy that you wish to delete and then click **Delete**.

VIEW MEDIA ASSOCIATED WITH A TRACKING POLICY

Required Capability: See Capabilities and Permitted Actions

To view the media associated with a Tracking Policy:

1. From the CommCell Browser, click the **VaultTracker Policies** icon under the **Policies** node.

   All the available Tracking Policies are displayed in the right pane of the CommCell Browser.
2. Right-click the Tracking Policy that you wish to view the associated media and click **View Media**.
3. The View Media dialog box, displays a list of media that satisfies the criteria defined in the Tracking Policy.

RUN A TRACKING POLICY

Required Capability: See Capabilities and Permitted Actions

To run a Tracking Policy:

1. From the CommCell Browser, click the **VaultTracker Policies** icon under the **Policies** node.

   All the available Tracking Policies are displayed in the right pane of the CommCell Browser.
2. Right-click the policy that you wish to run and then click **Run**.

When a Tracking Policy is initiated, the following are displayed in the CommCell Console:

- An Event Message is generated to indicate that the Tracking Policy has been successfully initiated.
- If the auto-acknowledge option is enabled in the Tracking Policy, the system will automatically acknowledge all pending actions associated with the media movement if both source and destination is a location. If the source is a library, the pending actions will be automatically acknowledged when the media is removed from the library.
- For jobs that require to be manually acknowledged, the Pending Actions are displayed on the right pane of the CommCell Browser, when you click the **Action** icon under **VaultTracker**.

You must record the status of the media as it goes through the various stages, as described in Monitor and Record the Status of a Media.

SCHEDULE A TRACKING POLICY

Required Capability: See Capabilities and Permitted Actions

To schedule a Tracking Policy:

1. From the CommCell Browser, click the **VaultTracker Policies** icon under the **Policies** node.

   All the available Tracking Policies are displayed in the right pane of the CommCell Browser.
2. Right-click the Tracking Policy that you wish to schedule and click **Create Schedule**.
3. Create the necessary schedules for the Tracking Policy, from the Schedule Details tab.
4. Click **OK** to save the schedule.

- Schedules for Tracking Policies honor holidays on the CommServe level.
- When the schedule for the Tracking Policy is initiated, the following are displayed in the CommCell Console:

  An Event Message is generated to indicate whether the Tracking Policy has been successfully initiated.
- If the auto-acknowledge option is enabled in the Tracking Policy, the system will automatically acknowledge all pending actions associated with the media movement if both source and destination is a location. If the source is a library, the pending actions will be automatically acknowledged when the media is removed from the library.
- For jobs that require to be manually acknowledged, the Pending Actions are displayed on the right pane of the CommCell Browser, when you click the **Action** icon under **VaultTracker**.
- Options to view, modify, delete or disable schedules are also available. See the following topics for more information:
  - View a Job Schedule
  - Modify a Job Schedule
  - Disable a Schedule
  - Delete a Job Schedule

EXPORT MEDIA USING THE EXPORT MEDIA WIZARD

Required Capability: Library Management

To export media from a library using the Export Media Wizard:

1. From the CommCell Browser, right-click the library from which you want to export media, and then click **Export Media**.

   OR

   The **Export Media Wizard** is displayed.
2. From the **Export Media** window in the **Export Media Wizard**, choose whether or not to use VaultTracker to export media.
   - If you choose to export media using VaultTracker, the **Export Media Wizard** guides you through the process of creating tracking policies, choosing media movement criteria, selecting destination and tracking options, etc.
   - If you choose not to export media using VaultTracker, the **Export Media Wizard** guides you through the process of exporting specific media using the **Export Media List**.

     You can also access the **Export Media Wizard** by right-clicking the media you wish to export in the **Media in Library** node and selecting **Export Media**. The **Export Media Wizard** is then displayed.

EXPORT MEDIA FROM A LIST USING VAULTTRACKER

Required Capability: See Capabilities and Permitted Actions

To export media from a list using VaultTracker:

1. Initiate an Export Media operation as described in Exporting Media From a List.

   An export media operation can be run immediately or scheduled using the scheduling options.
2. From the **Export Media List** dialog box, click **Advanced**.
3. From the Advanced Options dialog box, click the **Use VaultTracker for export** option.
4. Click the **Use Virtual Mail Slots** option to automatically move the media to a virtual mail slot in the library. Virtual mail slots are defined in the Library Properties (Media) tab.
5. Click the **Auto-acknowledge** option if you want the system to automatically acknowledge all Pending movement actions.
6. Select a **Container** if the media is added to a Container.
7. Click the **Track Transit** option and select the transit location from the list, to track the transit information. Transit locations can be entered using the Export Location Details dialog box.
8. Click **OK** to save the information.

- If the auto-acknowledge option is enabled, the system will automatically acknowledge all pending actions associated with the media movement if both source and destination is a location. If the source is a library, the pending actions will be automatically acknowledged when the media is removed from the library.
- If the auto-acknowledge option is not enabled, the Pending Actions are displayed on the right pane of the CommCell Browser, when you click the **Action** icon under **VaultTracker**.

You must record the status of the media as it goes through the various stages, as described in Monitor and Record the Status of a Media.

Set Automatic Tracking in a Tracking Policy

Required Capability: See Capabilities and Permitted Actions

➡ To Set Automatic Tracking in a Tracking Policy:

1. From the CommCell Browser, right-click the **VaultTracker Policies** icon under the **Policies** node.

   All available Tracking Policies are displayed in the right pane of the CommCell Browser.

2. Right-click the policy that you wish to modify and then click **Properties**.
3. From the **General** tab of the **Tracking Policy Details** dialog box click the **Auto acknowledge** option.
4. Click **OK** to save the information.

You can also enable the auto-acknowledge option for export media operations. See Initiate Media Movement After An Export Media Operation for step-by-step instructions.

Monitor and Record the Status of a Media

Required Capability: See Capabilities and Permitted Actions

➡ To monitor or record the status of a media:

1. From the CommCell Browser, click the **Actions** icon, under the **VaultTracker** icon.

   All the VaultTracker jobs with a pending action is displayed in the right-pane of the CommCell Browser.

2. Right click the action for which you wish to record the status and then click the appropriate movement action.

   If you wish to record the status for the individual media in the action, right-click the action and then click **Details**.

   From the Media Action Details dialog box, right-click the media for which you wish to record the status, and then click the appropriate movement action.

   Choose from the following options:

Status	Description
Reached Destination	Use this option to indicate that the media has reached its destination. Once the media reaches the destination, the history information for the media can be viewed in the Tracking History window.
Picked up	Use this option to indicate that the media has been picked up. This action is applicable only for media movement between two locations.
Return to Source	Use this option to return a media to its previous location.. This action is applicable only for media movement between two locations.
Abort	Use this option to abort the media movement operation at its current stage. This information will be added in the history.

Available status:

- When the media is at source, the following status can be recorded:

  If the current location of the media is inside the library, status cannot be recorded.

  If current location of the media is outside the library, the following status can be recorded: **Picked Up**, **Reached Destination**
- When the media is in the virtual mail slot, status cannot be recorded.
- When the media is in transit, the following status can be recorded:

  If the destination is an export location, the **Reached Destination** status can be recorded.

  When the destination is a library, status cannot be recorded.

  If the source and destination are an export location, the **Return to Source** and **Reached Destination** status can be recorded.

The status options available for an action (as opposed to the status options available for a media in the Media Action Details dialog box) is the combination of all available commands for all the media associated with the action.

View the Tracking History

Required Capability: See Capabilities and Permitted Actions

To view the tracking history:

1. From the CommCell Browser, right-click the **Actions** icon under **VaultTracker**, and then click **Tracking History**.
2. Select the necessary filter criteria from the Media Movement Filter Criteria dialog box.
3. The Tracking History window displays the history information associated with media movement.

   If necessary, you can roll back or delete an action as described in Roll Back an Action in the Tracking History and Delete an Action in the Tracking History.

VaultTracker history information is automatically pruned by VaultTracker after 90 days.

DELETE ACTION IN THE TRACKING HISTORY

Required Capability: See Capabilities and Permitted Actions

To delete an action in the tracking history:

1. From the CommCell Browser, right-click the **Actions** icon under the **VaultTracker**, and then click **Tracking History**.
2. The Tracking History window displays the history information associated with media movement.
3. Right-click the action you wish to delete and then click **Delete**.

   The VaultTracker action is deleted from the history.

ROLL BACK AN ACTION IN THE TRACKING HISTORY

Required Capability: See Capabilities and Permitted Actions

To delete an action in the tracking history:

1. From the CommCell Browser, right-click the **Actions** icon under the **VaultTracker**, and then click **Tracking History**.
2. The Tracking History window displays the history information associated with media movement.
3. Right-click the action you wish to roll back and then click **Roll Back**.

   The VaultTracker action is rolled back from the history.

Roll back option will not be available in the following situations:

- When the media movement history has a library as the source or destination location.
- When the media movement history was a failure.

ADD/MODIFY A LOCATION

Required Capability: See Capabilities and Permitted Actions

To add or modify a location:

1. From the CommCell Browser, right-click the **Locations** icon under the **Storage Resources** level, and then click **New Location**.
2. From the Export Location Details dialog box, enter the following:

   The name of the location.

   Select whether the location is **Stationary** or **Transit** location.

   Provide a brief description (optional) for the location.
3. Click **OK**.

   The new location is added.

Locations can also be added by typing a location name in the VaultTracker operations. For example, Tracking Policy, Export Media operation, etc.

Delete a Location

Before You Begin

- Ensure that the export location you wish to delete is not associated with a Tracking Policy or pending action. Also ensure that no media currently resides in the location.

Required Capability: See Capabilities and Permitted Actions

To delete a location:

1. From the CommCell Browser, right-click the **Locations** icon under **Storage Resources**.
2. All the available location are displayed on the right pane.
3. Right-click the location and then click **Delete**.
4. Click **Yes** in the Confirm prompt.

   The location is deleted.

Back To Top

VaultTracker® Enterprise Feature

Topics | How To | How Do I | Support | Related Topics

OVERVIEW

The **VaultTracker® Enterprise Feature** license provides the capability to track media movement between several locations. In addition to the standard VaultTracker® features, it also provides several advanced capabilities. The following sections describe the features and capabilities specific to **the VaultTracker Enterprise Feature**.

The VaultTracker license provides the capability to track media movement between two locations. It is also used to export media. For information on the specific VaultTracker features and capabilities, see VaultTracker Feature.

For information on license requirements, see VaultTracker® Licenses in License Administration.

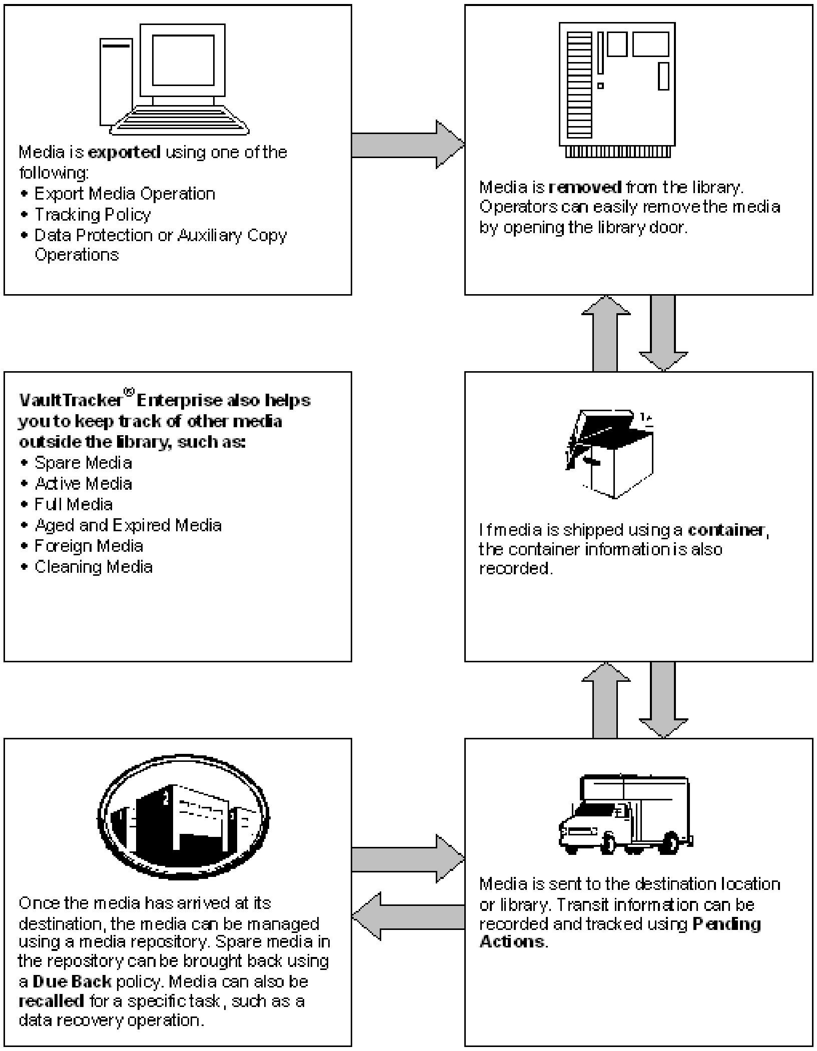
MANAGING MEDIA

The VaultTracker® Enterprise Feature provides the facility to manage media that are removed from a library and stored in offsite locations. In practical terms, VaultTracker Enterprise feature provides the following capabilities in your day-to-day operations:

- Identifies media that must be sent off-site for storage or brought back from off site locations.
- Automatically moves the media in sequence in the library and provides a pick-up list for the operators.
- Facility to identify and track media during transit.
- Facility to record and track containers when the media is stored and moved using containers.
- Facility to record and track the movement of media not used by all MediaAgents or Foreign Media.

The following diagram provides an overview of VaultTracker Enterprise Feature:

Moving and Tracking Media using the VaultTracker® Enterprise Feature



Media is **exported** using one of the following:
- Export Media Operation
- Tracking Policy
- Data Protection or Auxiliary Copy Operations

Media is **removed** from the library. Operators can easily remove the media by opening the library door.

If media is shipped using a **container**, the container information is also recorded.

Media is sent to the destination location or library. Transit information can be recorded and tracked using **Pending Actions**.

Once the media has arrived at its destination, the media can be managed using a media repository. Spare media in the repository can be brought back using a **Due Back** policy. Media can also be **recalled** for a specific task, such as a data recovery operation.

VaultTracker® Enterprise also helps you to keep track of other media outside the library, such as:
- Spare Media
- Active Media
- Full Media
- Aged and Expired Media
- Foreign Media
- Cleaning Media

How to Use the VaultTracker® Enterprise Feature

The following section describes the possible steps involved in tracking media using VaultTracker® Enterprise:

1. Initiate the VaultTracker feature process by exporting the media using VaultTracker enterprise feature.
    - For media that should be exported immediately, you can export the media from a list of available media with the VaultTracker feature enabled.
    - For media that should be exported once certain criteria are met, you can define one or more Tracking Policies.

      A Standard Tracking Policy can track the movement of media between any source and destination.

      A Due Back policy can track the movement of spare media residing in an off-site location.

- For media that should be exported at the completion of a data protection or auxiliary copy operation, you can configure the operation to export the media using the VaultTracker feature once the operation has completed.

2. Once the Export Media operation has been initiated, you can remove the media from the library. Qualifying media can either be ejected from the library's mail-slot or can be sorted into virtual mail slots that are defined in the library, so that these media can be easily removed by opening the library door.

   If media is moved to an off-site location, containers can be created.

3. While the media is in transit, you can track and acknowledge the status of the media using Pending Actions.
   - Use Manual Acknowledgement to track the media manually in the CommCell® Browser.
   - Use Automatic Acknowledgement to automatically acknowledge all pending actions associated with the media as long as the source and destination are locations.
4. Create one or more alerts to provide notification of movement actions as they are completed.
5. If an exported media is needed for a data recovery operation, the media can be recalled using the Recall Media feature. See Recall Media for more information on recalling media.
6. Iron Mountain customers can generate the necessary reports in the appropriate format and either directly mail them out on a scheduled basis or save them to a target location.
7. View information about the media managed by VaultTracker Enterprise feature by generating a Tracking Report, which can include pending actions, spare media that are due back, and media associated with a Tracking Policy.

The following sections describe each of these possible steps in depth.

EXPORTING MEDIA USING VAULTTRACKER® ENTERPRISE FEATURE

You can export media using the VaultTracker Feature software and VaultTracker Enterprise Feature in the following ways:

- using the **Export Media Wizard**
- using the **Export Media from a List** feature
- using **VaultTracker Policies**
- after Data Protection and Auxiliary Copy Operations (VaultTracker Enterprise Feature only)

All three methods provide the necessary options to run the export operation immediately or schedule the export operation to run for a later time.

You can configure the number of times an export operation must retry before it is aborted, and the retry interval minutes using the **Export Operation Retry Count** and the **VaultTracker feature export retry interval in minutes** options from the Media Management Configuration (Service Configuration) dialog box available in the **Control Panel**.

The following sections discuss the various export media options in depth.

EXPORTING MEDIA USING THE EXPORT MEDIA WIZARD

The **Export Media Wizard** provides the capability to quickly export one or more media from a library. This wizard is useful if you know the library containing the media you wish to export, as well as the media to be exported. You can choose to export media in 2 ways:

- using the VaultTracker/VaultTracker Enterprise feature, which provides all the options you need create tracking policies.
- from a list of available media in the library, from which you can select the appropriate media to be exported. The media will then be automatically placed in the appropriate mail slot for removal.

The Export Media Wizard is accessible at the **Library** and **Media in Library** levels in the CommCell® Console. See Export Media using the Export Media Wizard for step-by-step instructions.

EXPORTING MEDIA FROM A LIST

Media can be selected from a list of media and exported. This is useful when you wish to export several media at the same time and know either the media's barcode, or slot number in which the media resides. This task can be performed from the following levels in the CommCell® Console:

- **Media List** dialog box which appears when you select the **View Media** option. This dialog box can be accessed by right-clicking a Storage Policy copy.
- **Media List** dialog box which appears when you select the **Change Data Path** option. This dialog box can be accessed by right-clicking a Storage Policy copy.
- **Media List** dialog box which appears when you select the **Media Not Copied** option. This dialog box can be accessed by right-clicking a Storage Policy and Storage Policy copy.

Once the media to be exported is selected, you can choose to use the VaultTracker feature to track the export operation by clicking on the **Advanced** button in the Export Media List dialog box. A Tracking policy can be created to export media based on the selected criteria.

See Export Media from a List using VaultTracker Feature for step-by-step instructions.

EXPORTING MEDIA USING TRACKING POLICIES

Tracking Policies help you to define what media must be moved, where it must be moved to, and when it should be moved. This is useful if you wish to schedule routine exports of media that have satisfied certain criteria.

Tracking Policies can be used to track regular media movements, such as when media is shipped from a library to off-site storage, media repository, or shipment of media between 2 locations, etc. Once a policy is created, you can view the media associated with that policy by right-clicking on the policy and selecting **View Media**.

Two types of tracking policies are available, described below, which are created using the **VaultTracker Enterprise Policy Wizard**.

STANDARD POLICIES	A standard policy can be created to track the movement of media between any source and any destination, including: ● Library to location ● Location to location ● Location to library ● Library to library
DUE BACK POLICIES	A Due Back policy can be created to track the movement of spare media stored in an off-site location.

When creating a policy, you can:

- Schedule the policy to run at a later time if you anticipate changes being made to the policy prior to media movement taking place. Policies can be scheduled to run daily, weekly, etc., if desired.
- Delay the export of the media, which creates a time gap between when the policy is run and when the media movement actions actually start. This provides time for you to create and review a Vault Tracking Report with all the policy's actions detailed prior to any actions taking place. If any changes to the policy are required, you can perform these changes without aborting or rerunning an action.
- Temporarily stop an action by placing the export operation in a pending state for a specified amount of time. This is useful if you need to perform library maintenance or urgent data protection and recovery operations, but do not wish to abort or restart what has already been completed. You can manually restart the policy from the point it left off when the library is available, or you can set the policy to resume automatically at a specific time.

Once created, you can further facilitate Tracking Policies by right-clicking on the policy in the CommCell® Console:

- **Run** the policy if you wish to initiate the policy without further delays or changes to the policy.
- **Clone** the policy to create an exact duplicate of the policy that retains all of the properties of the original policy. Once created, you can edit the properties of the policy, if necessary. This saves you the time of creating a new policy manually. (See Cloning Policies for more information.)
- Change the **Properties** of a policy if you wish to make changes to the configuration of the policy while it is still in the pending state.

For step-by-step instructions on creating and managing tracking policies, see the following:

- Create a Tracking Policy
- Clone a Tracking Policy
- Modify a Tracking Policy
- Delete a Tracking Policy
- View Media Associated with a Tracking Policy
- Run a Tracking Policy
- Schedule a Tracking Policy

EXPORTING MEDIA AFTER DATA PROTECTION AND AUXILIARY COPY OPERATIONS

A media movement can also be triggered by a Data Protection or Auxiliary Copy operation, either scheduled, or performed immediately. Once the operation succeeds, the media movement operation will be triggered. These options are useful when media associated with a specific job has to be sent offsite, then the Data Protection or Auxiliary Copy schedule can be marked accordingly so that an action can be directly initiated upon successful completion of the job.

If media associated with a specific job has to be sent offsite, then the Data Protection or Auxiliary Copy schedule can be marked accordingly so that an action can be directly initiated upon successful completion of the job.

For step-by-step instructions, see the following:

- Export Media After a Data Protection Operation
- Export Media After an Auxiliary Copy Operation

See Also: Export Media

REMOVING MEDIA FROM THE LIBRARY

Once the export operation has been initialized, the media can then be removed from the library in the following ways:

- Use the virtual mail slot option to store the media in contiguous slots in the library, so that it can be easily removed by opening the library door.
- Can be ejected using the library mail slots.

VIRTUAL MAIL SLOTS

Virtual mail slots are a range of contiguous slots in the library that are used to store media that are to be moved out. Virtual mail slots provide the facility to open the library door and pick up the media to be moved from a pre-determined range of slots.

Virtual mail slots in a library can be defined from the **Library Properties** dialog box. You must also specify whether VaultTracker® Enterprise must use the virtual mail slot in the Tracking Policy, Data Protection, Auxiliary Copy or Export Media operations.

Media moved to the virtual mail slots are marked as **Exportable**. An option to use the media in virtual mail slots for data protection operations, is also provided in the **Library Properties** dialog box.

Virtual mail slots are not supported for IP-based libraries, such as libraries attached to an ACSLS Server, ADIC libraries attached to SDLC, etc.

LIBRARY MAIL SLOTS

If you do not setup the virtual mail slots in the library, the media will be automatically exported using the library's mail slots.

MOVING MEDIA USING CONTAINERS

When containers are used to ship out media, the container information can be added as an additional attribute of the media information. This information will be useful to identify the container in which the media is located when the media is recalled.

When the capacity of a container has been reached, any remaining media is automatically carried over to the next available container defined in the Tracking Policy.

CREATING CONTAINERS

Containers can be created using the following methods:

- Containers can be automatically created from a Tracking Policy, using an automated mechanism to generate the container names. If this is established, a container will be automatically created whenever the Tracking Policy is run and all the location for all the media associated with the job will be automatically set to the associated container.

  See Establish Automatic Container Generation in a Tracking Policy for step-by-step instructions.

- Containers can also be manually created from the CommCell® Browser by right-clicking the **Containers** icon, under **VaultTracker**, and then clicking **New Container**.

  See Add/Modify a Container for step-by-step instructions.

Once the container is created, you can **Move**, **Remove**, **Delete**, and **Recall** all media associated with that container by right-clicking on the container in the CommCell Browser and selecting the desired option. You can also view/edit the container's **Properties**.

ASSOCIATING CONTAINER INFORMATION TO THE MEDIA

For media that are not automatically associated with a container, (as explained in the preceding sections), there are several ways of associating the container information. They are:

- When you record the Pending Action as Reached Destination, you will be provided with the option to set a container if necessary.

- You can set the container for any Pending Action that are displayed in the right-pane of the CommCell® Browser, when you click the Actions icon under **VaultTracker**.
- Containers can also be associated with media displayed in the Exported Media pool. This can be done in two ways:
  - You can individually associate a container for a specific media by opening and **Media Properties** and selecting a container as the location for the media.
  - Set the container for all media in the Exported Media pool, by right-clicking the **Exported Media** icon displayed under **Media By Location** and then clicking the **Set Container** option.

See Add Media to a Container for step-by-step instructions.

LOCATING THE CONTAINER ASSOCIATED WITH A MEDIA

The contents of a container can be viewed using the **View Media** option associated with the container in the CommCell Console. See Display the Media available in a Container for step-by-step instructions.

You can also generate a Tracking Report or Media Information report as appropriate. The container associated with the specific media is displayed in these reports.

PRUNING CONTAINER INFORMATION

VaultTracker® Enterprise prunes empty container details based on the number of days established in the **Container cleanup interval days** option from the **Media Management Configuration (Service Configuration)** dialog box available in the **Control Panel**.

Container information can also be manually deleted from the policy when the container is no longer needed. See Delete Container Information for step-by-step instructions.

SETTING CONTAINER INFORMATION USING BARCODES

The `setMediaLocation` utility, which can be obtained from the software Resource Pack, allows you to set container information for media using the media's barcode. This is useful if you wish to incorporate existing barcode scanning capabilities with media movement operations performed with VaultTracker® Enterprise Feature. See Resource Pack for more information.

RECORDING PENDING ACTIONS

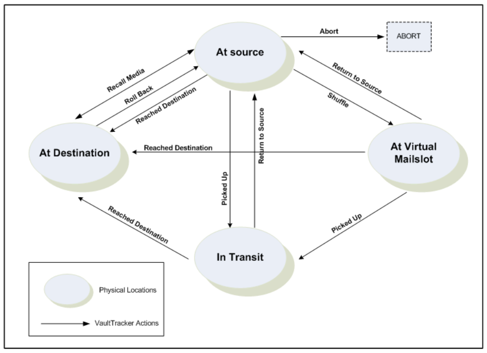
Once media is removed from the library, all media movement outside the library must be recorded to track the operation. Such outside media movements are referred to as **Pending Actions**. Once an action is initiated, the media will be displayed in the reconciliation report.

The following list provides links to diagrams that depict the various types of media movements and the options provided for recording pending actions:

- Media Movement between 2 Locations
- Media Movement from a Library to Location
- Media Movement from a Location to a Library
- Media Movement between 2 Libraries

The following pending actions can be recorded:

- **Picked up** - This option should be used to set the media location as *In Transit*, when the source is a location. (In the case of a library, this option will be automatically performed when the media is removed from the source library.)
- **Reached Destination** - This option should be used to indicate that the media has reached its destination. The pending action is considered to be completed and the pending action information is displayed in the **Tracking History**. If the final destination is a library, this option will be automatically performed when the media is detected in the destination library.
- **Return to Source** - This option should be used to reset media location to the source location. This option is valid only when:
  - The media is in the in-transit state.
  - When the source is a location. (not a library)
- **Abort** - Aborts the pending action.
- **Suspend** - Temporarily discontinues all media movement for a specified amount of time. The media movement can be resumed manually or at a specified time.
- **Resume** - Media movement continues when a suspension has been lifted by either manually resuming the action or when the specified **Suspend** time has expired.
- **Set Container** - Assign a specific container to the selected policy.



- **Recall Media** - Media that is being brought back to the source location for a specific task, such as a data recovery operation.
- **Quit Time** - Specify the amount of time to elapse for the action to abort. This is also configurable in the Media Management Configuration (Service Configuration) dialog box.

The diagram on the right provides a summary of all pending actions.

You can view the pending actions in the CommCell® Browser by right-clicking the **VaultTracker** icon under the **Storage Resources** icon, and then clicking **Actions**. All pending actions are displayed on the right-hand pane.

ACKNOWLEDGING PENDING ACTIONS

VaultTracker® Enterprise Feature provides two ways of acknowledging pending actions:

- Manual Acknowledgement
- Automatic Acknowledgement

These are explained in the following sections.

MANUAL ACKNOWLEDGMENT

When you run a data protection operation, auxiliary copy operation, Export Media operation, or Tracking Policy with the auto-acknowledge option disabled, you must manually acknowledge the media movement actions. You can record the pending action either for all media associated with a specific movement, or for individual media associated with a specific movement.

There are two methods with which you can manually acknowledge pending actions:

1. **Pre-acknowledge**: All pending actions can be acknowledged assuming that the tapes will get to the destination.

   You can then generate a Media Information report, which sorts the media based on the export location. This report can then be sent to an offsite person/agency to verify that the contents matches the information in VaultTracker® Enterprise.
2. **Post-acknowledge**: The Tracking Report with the **Reconciliation** option enabled can be generated. All media which are in transit are listed. Once a confirmation from offsite is received, all Pending Actions can be acknowledged.

See Monitor and Record the Status of a Media for step-by-step instructions.

AUTOMATIC ACKNOWLEDGMENT

When you create a Tracking Policy, you can enable the Auto-Acknowledge option within the policy. When such a policy is run, the system will automatically acknowledge all pending actions associated with the media movement if both source and destination is a location. If the source is a library, the pending actions will be automatically acknowledged when the media is removed from the library.

Note that the automatic acknowledgement option can be enabled (or disabled) for a Tracking Policy and Media Export operations. Automatic acknowledgement is not available for Data Protection and Auxiliary copy operations.

See Set Automatic Tracking in a VaultTracker Policy for step-by-step instructions.

VIEWING TRACKING HISTORY

Once all the pending actions are recorded, the VaultTracker® Enterprise Feature automatically catalogs the information in the Tracking History. VaultTracker® Enterprise history can be viewed from the CommCell® Browser by right-clicking the **Actions** icon under **VaultTracker**, and then clicking **View History**. Filter options for viewing the history are also provided.

If you would like the information to be displayed in the Actions pane before it is moved to the history information, you can establish a display time using the **Time in hours to show the vault tracker history in actions pane** option from the **Media Management Configuration (Service Configuration)** dialog box available in the **Control Panel**.

See View the Tracking History for step-by-step instructions:

ROLLING BACK AN ACTION

The **Roll Back** option can be performed if both the source and destination locations were export locations and the media is listed in the history information after being marked as reached destination. This option provides the opportunity to rollback a wrong location change.

See Roll Back an Action in the Tracking History for step-by-step instructions.

DELETING AN ACTION

You can **Delete** a pending action history or delete individual media action history of a pending action.

See Delete an Action in the Tracking History for step-by-step instructions.

PRUNING TRACKING HISTORY

Tracking History information is by default pruned after 90 days. If necessary this value can be modified using the **Days to keep VaultTracker records** option from the **Media Management Configuration (Vault Tracker Configuration)** dialog box available in the **Control Panel**.

MANAGING MEDIA REPOSITORY

Media Repository provides a way of keeping track and managing media that are stored in outside storage locations. For example, Media Repository provides the facility to manage spare and new media, foreign media or media not used by the MediaAgents in this CommCell® group, expired media, etc. that reside outside the libraries.

A media repository can be created from the CommCell Browser by right-clicking the **Media Repository** icon, under **VaultTracker**, and then clicking **Add Shelf**. When you create a shelf in a media repository, the various Media Groups are automatically created by default. If necessary you can add additional media groups to the shelf. You must assign a default media type for the various groups within the media repository. You can then add media available in the media repository, using either specific barcodes or a range of barcodes as appropriate.

Note that a Media Repository can be specified as the target location when media is tracked from VaultTracker® Enterprise.

See the following for step-by-step instructions:

- Add a Media Repository
- Specify the Default Media Type for a Media Group in the Media Repository
- Add Media to a Media Group in the Media Repository

RECORDING LOCATIONS

An option to add all locations, including stationary and transit locations has been provided. This includes the facility to modify or delete existing locations.

See the following for step-by-step instructions:

- Add/Modify a Location
- Delete a location

SETTING LOCATION INFORMATION USING BARCODES

The `setMediaLocation` utility, which can be obtained from the software Resource Pack, allows you to set location information for media using the media's barcode. This is useful if you wish to incorporate existing barcode scanning capabilities with media movement operations performed with VaultTracker® Enterprise. See Resource Pack for more information.

ALERTS

Several alerts can be configured where necessary. For a detailed description of these alerts, see Media Management in Alerts and Monitoring.

Additionally, you can configure alerts for Recall Media operations. See Alerts Configuration in Recall Media for more information.

See Configure Global Alerts for step-by-step instructions on creating alerts.

A time interval for generating VaultTracker® alerts can be established using the **Interval (Minutes) between VaultTracker® alerts** option from the **Media Management Configuration (Service Configuration)** dialog box available in the **Control Panel**.

Recall Media

The Recall Media feature provides the facility to temporarily bring media back from an export location for a specific operation and return the media to the export location when the operation is complete. This capability is useful if you have exported media to another location with the intention of keeping the media at the export location for an established period of time, but need to bring the media back from the export location for a specific purpose (such as a data recovery operation) prior to the original return date.

See Recall Media for more information.

Recording the Iron Mountain Customer Identification Number

You can record the unique Iron Mountain Customer Identification numbers for each Iron Mountain account provided to your enterprise. These numbers will be used by the CommServe to generate the reports that are requested in the Iron Mountain format.

See Add or Modify the Customer Identification Number for step-by-step instructions.

License Requirements

For information on license requirements, see VaultTracker® Licenses in License Administration.

Related Reports

VAULT TRACKING REPORT

The Vault Tracking Report can be generated to view information about media managed by the VaultTracker® feature, including pending actions, spare media that are due back, movement action history, and media related to a VaultTracker policy. Each Vault Tracking Report can be generated and saved in HTML, text, and Iron Mountain Report formats. Optionally, a style sheet can be selected to customize the XML output.

The **Reconciliation** option, if selected, will display all the tapes that are pending their arrival at the destination.

If the **Due Back** option is selected, the Tracking Report will display all spare media or media that will become spare media. The tracking report can be used without initiating actual actions. An option to filter media based on time range, storage policies and estimated retention time is also available.

For information on generating and using the Vault Tracking Report, see Vault Tracking Report.

MEDIA INFORMATION REPORT

The Media Information report can be generated by sorting the media based on the export location. This report can then be sent to an offsite person/agency to verify that the contents matches the information in the VaultTracker® feature.

Registry Keys Use Cases

Use the following registry keys to modify the default behavior for the VaultTracker® feature:

Registry Key(s)	Description
`VaultTrackerExportDelayTime`	This registry key introduces a delay time for scheduling a reconciliation report.
`VaultTrackerExportQuitTime`	This registry key forces the export of media to end after a certain amount of time.
`nKeepVTHistoryWithActionsForHours`	This registry key allows you to keep actions in the Media Action Details window for 15 minutes by default (time is configurable in this key).

Back to Top

VaultTracker® Enterprise Feature - How To

Topics | How To | How Do I | Support | Related Topics

Overview

Track Media using VaultTracker Feature and VaultTracker Enterprise Feature

Tracking Policies

Create a Tracking Policy

Clone a Tracking Policy

Modify a Tracking Policy

Delete a Tracking Policy

View Media Associated with a Tracking Policy

Run a Tracking Policy

Schedule a Tracking Policy

Export Media using VaultTracker

Export Media using the Export Media Wizard

Export Media From a List using VaultTracker

Export Media After a Data Protection Operation

Export Media After An Auxiliary Copy Operation

Pending Actions

Set Automatic Tracking in a Tracking Policy

Monitor and Record the Status of a Media

Virtual Mail Slot

Set up the Virtual Mail Slots in the Library

Tracking history

View the Tracking History

Delete an Action in the Tracking History

Roll Back an Action in the Tracking History

Export Locations

Add/Modify a Location

Delete a location

Media Repository

Add a Media Repository

Specify the Default Media Type for a Media Group in the Media Repository

Add Media to a Media Group in the Media Repository

Containers

Establish Automatic Container Generation in a Tracking Policy

Add/Modify a Container

Delete Container Information

Add Media to a Container

Display the Media available in a Container

Iron Mountain Customer Identification Number

Add or Modify the Customer Identification Number

TRACK MEDIA USING VAULTTRACKER FEATURE AND VAULTTRACKER ENTERPRISE FEATURE

Required Capability: See Capabilities and Permitted Actions

To track media using VaultTracker Feature and VaultTracker Enterprise Feature:

1. Create the list of media that must be tracked. This can be done in one of the following ways:
   - Create a Tracking Policy as described in Create a Tracking Policy.
   - Specify that media associated with a backup job must be exported and tracked as described in Export Media After a Date Protection Operation (VaultTracker Enterprise Feature only), Export Media After An Auxiliary Copy Operation (VaultTracker Enterprise Feature only), and Export Media from a List using VaultTracker.
2. If you have created a Tracking Policy, you must run or schedule the policy, as described in Run a Tracking Policy and Schedule a Tracking Policy.

   If necessary, you can you can view the media associated with a Tracking Policy as described in View Media Associated with a Tracking Policy.
3. Once the media movement is initiated, you must monitor and record the status of the media, as described in Monitor and Record the Status of a Media.
4. Once the media movement is completed, you can view the history information for the media, as described in View Tracking History.

CREATE A TRACKING POLICY

Required Capability: See Capabilities and Permitted Actions

To create a Tracking Policy:

1. From the CommCell Browser, right-click the **VaultTracker Policies** icon under the Policies node, and then click **New Tracking Policy**.
2. The **VaultTracker Policy** wizard guides you through the process of creating a new Tracking Policy.

- A regular Tracking policy can be created to export media based on the selected criteria.
- A due back Tracking policy can be created to track the movement of spare media, residing outside the library.
- Once created the Tracking Policy must be run or scheduled, as described in Run a Tracking Policy and Schedule a Tracking Policy.

CLONE A TRACKING POLICY

Required Capability: See Capabilities and Permitted Actions

To clone a tracking policy:

1. From the CommCell Browser, click the **VaultTracker Policies** icon under the **Policies** node.

   All the available Tracking Policies are displayed in the right pane of the CommCell Browser.
2. Right-click the policy that you wish to clone and then click **Clone**.
3. Type the name of the new policy in the **Enter Name box** of the **Clone VaultTracker Policy** dialog box. Click **OK**. The cloned Tracking Policy is displayed in the VaultTracker Policies level of the CommCell Browser.
4. Right-click the Tracking policy, and then click **Properties**. The **Tracking Policy Details** dialog box is displayed.
5. From the **General** tab, click the **Enable** check box. Click **OK**. The Tracking policy is now enabled and ready for use.

- You must enable a cloned Tracking policy after it is created.
- It is recommended that some of the options of the cloned Tracking policy is changed to avoid an exact duplication of the policy.

MODIFY A TRACKING POLICY

Required Capability: See Capabilities and Permitted Actions

To modify a tracking policy:

1. From the CommCell Browser, right-click the **VaultTracker Policies** icon under the **Policies** node.

   All available Tracking Policies are displayed in the right pane of the CommCell Browser.
2. Right-click the policy that you wish to modify and then click **Properties**.
3. Make the necessary changes in the **Tracking Policy Details** dialog box and then click **OK** to save the information.

Delete a Tracking Policy

Before You Begin

- Ensure that no pending actions are in progress for the tracking policy you wish to delete.

Required Capability: See Capabilities and Permitted Actions

To delete a tracking policy:

1. From the CommCell Browser, right-click the **VaultTracker Policies** icon under the **Policies** node.

   All the available Tracking Policies are displayed in the right pane of the CommCell Browser.

2. Right-click the policy that you wish to delete and then click **Delete**.

View Media Associated with a Tracking Policy

Required Capability: See Capabilities and Permitted Actions

To view the media associated with a Tracking Policy:

1. From the CommCell Browser, click the **VaultTracker Policies** icon under the **Policies** node.

   All the available Tracking Policies are displayed in the right pane of the CommCell Browser.

2. Right-click the Tracking Policy that you wish to view the associated media and click **View Media**.
3. The View Media dialog box, displays a list of media that satisfies the criteria defined in the Tracking Policy.

Run a Tracking Policy

Required Capability: See Capabilities and Permitted Actions

To run a Tracking Policy:

1. From the CommCell Browser, click the **VaultTracker Policies** icon under the **Policies** node.

   All the available Tracking Policies are displayed in the right pane of the CommCell Browser.

2. Right-click the policy that you wish to run and then click **Run**.

When a Tracking Policy is initiated, the following are displayed in the CommCell Console:

- An Event Message is generated to indicate that the Tracking Policy has been successfully initiated.
- If the auto-acknowledge option is enabled in the Tracking Policy, the system will automatically acknowledge all pending actions associated with the media movement if both source and destination is a location. If the source is a library, the pending actions will be automatically acknowledged when the media is removed from the library.
- For jobs that require to be manually acknowledged, the Pending Actions are displayed on the right pane of the CommCell Browser, when you click the **Action** icon under **VaultTracker**.

You must record the status of the media as it goes through the various stages, as described in Monitor and Record the Status of a Media.

Schedule a Tracking Policy

Required Capability: See Capabilities and Permitted Actions

To schedule a Tracking Policy:

1. From the CommCell Browser, click the **VaultTracker Policies** icon under the **Policies** node.

   All the available Tracking Policies are displayed in the right pane of the CommCell Browser.

2. Right-click the Tracking Policy that you wish to schedule and click **Create Schedule**.
3. Create the necessary schedules for the Tracking Policy, from the Schedule Details tab.
4. Click **OK** to save the schedule.

- Schedules for Tracking Policies honor holidays on the CommServe level.
- When the schedule for the Tracking Policy is initiated, the following are displayed in the CommCell Console:

  An Event Message is generated to indicate whether the Tracking Policy has been successfully initiated.
- If the auto-acknowledge option is enabled in the Tracking Policy, the system will automatically acknowledge all

pending actions associated with the media movement if both source and destination is a location. If the source is a library, the pending actions will be automatically acknowledged when the media is removed from the library.

- For jobs that require to be manually acknowledged, the Pending Actions are displayed on the right pane of the CommCell Browser, when you click the **Action** icon under **VaultTracker**.
- Options to view, modify, delete or disable schedules are also available. See the following topics for more information:
  - View a Job Schedule
  - Modify a Job Schedule
  - Disable a Schedule
  - Delete a Job Schedule

EXPORT MEDIA USING THE EXPORT MEDIA WIZARD

Required Capability: Library Management

To export media from a library using the Export Media Wizard:

1. From the CommCell Browser, right-click the library from which you want to export media, and then click **Export Media**.

   OR

   The **Export Media Wizard** is displayed.

2. From the **Export Media** window in the **Export Media Wizard**, choose whether or not to use VaultTracker to export media.
   - If you choose to export media using VaultTracker, the **Export Media Wizard** guides you through the process of creating tracking policies, choosing media movement criteria, selecting destination and tracking options, etc.
   - If you choose not to export media using VaultTracker, the **Export Media Wizard** guides you through the process of exporting specific media using the **Export Media List**.

     You can also access the **Export Media Wizard** by right-clicking the media you wish to export in the **Media in Library** node and selecting **Export Media**. The **Export Media Wizard** is then displayed.

EXPORT MEDIA FROM A LIST USING VAULTTRACKER

Required Capability: See Capabilities and Permitted Actions

To export media from a list using VaultTracker:

1. Initiate an Export Media operation as described in Exporting Media From a List.

   An export media operation can be run immediately or scheduled using the scheduling options.

2. From the **Export Media List** dialog box, click **Advanced**.
3. From the Advanced Options dialog box, click the **Use VaultTracker for export** option.
4. Click the **Use Virtual Mail Slots** option to automatically move the media to a virtual mail slot in the library. Virtual mail slots are defined in the Library Properties (Media) tab.
5. Click the **Auto-acknowledge** option if you want the system to automatically acknowledge all Pending movement actions.
6. Select a **Container** if the media is added to a Container.
7. Click the **Track Transit** option and select the transit location from the list, to track the transit information. Transit locations can be entered using the Export Location Details dialog box.
8. Click **OK** to save the information.

- If the auto-acknowledge option is enabled, the system will automatically acknowledge all pending actions associated with the media movement if both source and destination is a location. If the source is a library, the pending actions will be automatically acknowledged when the media is removed from the library.
- If the auto-acknowledge option is not enabled, the Pending Actions are displayed on the right pane of the CommCell Browser, when you click the **Action** icon under **VaultTracker**.

You must record the status of the media as it goes through the various stages, as described in Monitor and Record the Status of a Media.

EXPORT MEDIA AFTER A DATA PROTECTION OPERATION

Required Capability: See Capabilities and Permitted Actions

To export media after a data protection operation:

1. From the CommCell Browser, right-click the subclient for which you wish to perform a data protection operation, and then click **Backup/Migrate** from the shortcut menu.

   Data Protection operations can be initiated immediately or scheduled using the scheduling options.

2. From the **Backup Options/Migrate Options** dialog box, select the necessary options.
3. Click **Advanced**.
4. From the **Advanced Backup Options/Advanced Migration Options** dialog box, click the **Export Media after the job finishes** option.
5. If necessary, select the option to **Exclude Media Not Copied**.
6. If necessary, select the necessary **Media Status**.
7. Select the **Export Location** from the list. Export locations can be entered using the Export Location Details dialog box.
8. Click the **Track Transit** option and select the transit location from the list, to track the transit information. Transit locations can be entered using the Export Location Details dialog box.
9. Click the **Use Virtual Mail Slots** option to automatically move the media after the data protection operation, to a virtual mail slot in the library. Virtual mail slots are defined in the Library Properties (Media) tab.
10. If you wish to filter media based on its retention, select the appropriate option.
11. Click **OK** to save the information.

Once the data protection operation completes, the Pending Actions (for tracking the associated media) are displayed on the right pane of the CommCell Browser, when you click the **Action** icon under **VaultTracker**.

You must record the movement action as described in Monitor and Record the Status of a Media.

Export Media After an Auxiliary Copy Operation

Required Capability: See Capabilities and Permitted Actions

To export media after an auxiliary copy operation:

1. From the CommCell Browser, right-click the storage policy for which you want to perform an auxiliary copy and then click **Auxiliary Copy**.

   Auxiliary Copy operations can be initiated immediately or scheduled using either the scheduling options or a Schedule Policy.

2. From the **Auxiliary Copy** dialog box, select the necessary options.
3. Click **Vault Tracking**.
4. From the Select Vault Tracking Options dialog box, click the **Export Media after the job finishes** option.
5. If necessary, select the option to **Exclude Media Not Copied**.
6. If necessary, select the necessary **Media Status**.
7. Select the **Export Location** from the list. Export locations can be entered using the Export Location Details dialog box.
8. Click the **Track Transit** option and select the transit location from the list, to track the transit information. Transit locations can be entered using the Export Location Details dialog box.
9. Click the **Use Virtual Mail Slots** option to automatically move the media after the Auxiliary Copy operation, to a virtual mail slot in the library. Virtual mail slots are defined in the Library Properties (Media) tab.
10. If you wish to filter media based on its retention, select the appropriate option.
11. Click **OK** to save the information.

Once the Auxiliary Copy operation completes, the Pending Actions (for tracking the associated media) are displayed on the right pane of the CommCell Browser, when you click the **Action** icon under **VaultTracker**.

You must record the movement action as described in Monitor and Record the Status of a Media.

SET AUTOMATIC TRACKING IN A TRACKING POLICY

Required Capability: See Capabilities and Permitted Actions

To Set Automatic Tracking in a Tracking Policy:

1. From the CommCell Browser, right-click the **VaultTracker Policies** icon under the **Policies** node.

   All available Tracking Policies are displayed in the right pane of the CommCell Browser.

2. Right-click the policy that you wish to modify and then click **Properties**.
3. From the **General** tab of the **Tracking Policy Details** dialog box click the **Auto acknowledge** option.
4. Click **OK** to save the information.

You can also enable the auto-acknowledge option for export media operations. See Initiate Media Movement After An Export Media Operation for step-by-step instructions.

MONITOR AND RECORD THE STATUS OF A MEDIA

Required Capability: See Capabilities and Permitted Actions

To monitor or record the status of a media:

1. From the CommCell Browser, click the **Actions** icon, under the **VaultTracker** icon.

   All the VaultTracker jobs with a pending action is displayed in the right-pane of the CommCell Browser.

2. Right click the action for which you wish to record the status and then click the appropriate movement action.

   If you wish to record the status for the individual media in the action, right-click the action and then click **Details**.

   From the Media Action Details dialog box, right-click the media for which you wish to record the status, and then click the appropriate movement action.

   Choose from the following options:

Status	Description
Reached Destination	Use this option to indicate that the media has reached its destination. Once the media reaches the destination, the history information for the media can be viewed in the Tracking History window.
Picked up	Use this option to indicate that the media has been picked up. This action is applicable only for media movement between two locations.
Return to Source	Use this option to return a media to its previous location.. This action is applicable only for media movement between two locations.
Abort	Use this option to abort the media movement operation at its current stage. This information will be added in the history.

Available status:

- When the media is at source, the following status can be recorded:

  If the current location of the media is inside the library, status cannot be recorded.

  If current location of the media is outside the library, the following status can be recorded: **Picked Up**, **Reached Destination**

- When the media is in the virtual mail slot, status cannot be recorded.
- When the media is in transit, the following status can be recorded:

  If the destination is an export location, the **Reached Destination** status can be recorded.

  When the destination is a library, status cannot be recorded.

  If the source and destination are an export location, the **Return to Source** and **Reached Destination** status can be recorded.

The status options available for an action (as opposed to the status options available for a media in the Media Action Details dialog box) is the combination of all available commands for all the media associated with the action.

SET UP THE VIRTUAL MAIL SLOTS IN THE LIBRARY

Required Capability: See Capabilities and Permitted Actions

To setup the virtual mail slots in the library:

1. From the CommCell Browser, right-click the library for which you wish to setup the virtual slots, and then click **Properties**.
2. Click the Media tab.
3. Click the **Virtual mail slot for export** option.
4. Enter the starting slot number that must be used for storing media in the virtual mail slot in the **Starts From** box.
5. Specify whether the direction that must be used from the starting slot number. (The options are UP and Down.)
6. Click **OK** to save the information.

To use the virtual mail slot, the VaultTracker job must have the Use Virtual Mail Slot option enabled. You can enable this option in one of the following dialog boxes:

- Selecting the **Use Virtual Mail Slots for export in source libraries** option in the Tracking Policy from the Tracking Policy Details (Criteria) dialog box.
- Selecting the **Use Virtual Mail Slots** option for a backup job, from the **Advanced Backup Options** dialog box.
- The MediaAgent does not support the creation of virtual mail slots for blind libraries and libraries attached to an ACSLS server.

VIEW THE TRACKING HISTORY

Required Capability: See Capabilities and Permitted Actions

To view the tracking history:

1. From the CommCell Browser, right-click the **Actions** icon under **VaultTracker**, and then click **Tracking History**.
2. Select the necessary filter criteria from the Media Movement Filter Criteria dialog box.
3. The Tracking History window displays the history information associated with media movement.

   If necessary, you can roll back or delete an action as described in Roll Back an Action in the Tracking History and Delete an Action in the Tracking History.

VaultTracker history information is automatically pruned by VaultTracker after 90 days.

DELETE ACTION IN THE TRACKING HISTORY

Required Capability: See Capabilities and Permitted Actions

To delete an action in the tracking history:

1. From the CommCell Browser, right-click the **Actions** icon under the **VaultTracker**, and then click **Tracking History**.
2. The Tracking History window displays the history information associated with media movement.
3. Right-click the action you wish to delete and then click **Delete**.

   The VaultTracker action is deleted from the history.

ROLL BACK AN ACTION IN THE TRACKING HISTORY

Required Capability: See Capabilities and Permitted Actions

To delete an action in the tracking history:

1. From the CommCell Browser, right-click the **Actions** icon under the **VaultTracker**, and then click **Tracking History**.
2. The Tracking History window displays the history information associated with media movement.
3. Right-click the action you wish to roll back and then click **Roll Back**.

   The VaultTracker action is rolled back from the history.

Roll back option will not be available in the following situations:

- When the media movement history has a library as the source or destination location.
- When the media movement history was a failure.

Add/Modify a Location

Required Capability: See Capabilities and Permitted Actions

To add or modify a location:

1. From the CommCell Browser, right-click the **Locations** icon under the **Storage Resources** level, and then click **New Location**.
2. From the Export Location Details dialog box, enter the following:

   The name of the location.

   Select whether the location is **Stationary** or **Transit** location.

   Provide a brief description (optional) for the location.
3. Click **OK**.

   The new location is added.

Locations can also be added by typing a location name in the VaultTracker operations. For example, Tracking Policy, Export Media operation, etc.

Delete a Location

Before You Begin

- Ensure that the export location you wish to delete is not associated with a Tracking Policy or pending action. Also ensure that no media currently resides in the location.

Required Capability: See Capabilities and Permitted Actions

To delete a location:

1. From the CommCell Browser, right-click the **Locations** icon under **Storage Resources**.
2. All the available location are displayed on the right pane.
3. Right-click the location and then click **Delete**.
4. Click **Yes** in the Confirm prompt.

   The location is deleted.

Add a Media Repository

To add a media repository:

1. From the CommCell Browser, right-click the **Media Repository** icon under **VaultTracker**, and then click **Add Shelf**.
2. From the **New Shelf** dialog box, enter the name.
3. Click **OK**.

   The media repository is added.

Specify the Default Media Type for a Media Group in the Media Repository

To Specify the Default Media Type for a Media Group in the Media Repository:

1. From the CommCell Browser, right-click the media group under the appropriate Media Repository, and then click **Properties**.
2. From the appropriate Group Properties dialog box, select the Media Type from the Default Media Type list.
3. Click **OK**.

Add Media to a Media Group in the Media Repository

Before You Begin

- Ensure that you specify the media type for the media group as described in Specify the Default Media Type for a Media Group in the Media Repository.

To Add Media to a Media Group in the Media Repository:

1. From the CommCell Browser, right-click the media group under the appropriate Media Repository, and then click **Add Media**.
2. You can choose to add specific media using the **By Barcodes** option or add a range of media using the **By Range** option.
3. If you choose the Barcode option, the **Media By Barcode** dialog box is displayed.

   Enter the barcodes associated with the media in the repository in the Barcodes list.

   If necessary, select an Export Location.

   Click **OK**. The specified barcodes are added and displayed in the CommCell Browser.
4. If you choose the Range option, the **Media By Pattern** dialog box is displayed.

   Enter the range of barcodes using `<NUMBERSTART>` followed by barcode pattern. For example to add media using the barcode pattern 100, you must specify `<NUMBERSTART>100`.

   Enter the number of media that must be added. (The system will sequentially add the numbers to the specified barcode pattern. For example, if you add 4 media, media with barcodes `100`,`101`, `102` and `103` will be added.

   If necessary, select an Export Location.

   Click **OK**. The specified barcodes are added and displayed in the CommCell Browser.

ESTABLISH AUTOMATIC CONTAINER GENERATION IN A TRACKING POLICY

Required Capability: See Capabilities and Permitted Actions

To Establish Automatic Container Generation in a VaultTracker Policy:

1. From the CommCell Browser, right-click the **VaultTracker Policies** icon under the **Policies** node.

   All available Tracking Policies are displayed in the right pane of the CommCell Browser.
2. Right-click the policy that you wish to modify and then click **Properties**.
3. Click the **Destination** tab and then click **Container**.
4. From the Container Definition dialog box, click the **Container name pattern** option.
5. Select the label and then click **Add Token**. The selected label is displayed in the box at the bottom of the region.
6. Click **OK** to save the information.

The above container name pattern can also be established when the Tracking Policy is created using the **VaultTracker Policy** wizard.

ADD/MODIFY A CONTAINER

Required Capability: See Capabilities and Permitted Actions

To add/modify a container:

1. From the CommCell Browser, right-click the **Container** icon under **VaultTracker**, and then click **New Containers**.
2. From the Container Details dialog box, enter the following:

   The name of the container.

   The maximum number of media that the container can hold.

   A brief description (optional) for the container.
3. Click **OK**.

   The new container is added.

DELETE CONTAINER INFORMATION

Before You Begin

- Ensure that the container that you wish to delete does not have any media assigned to it. (See Add Media to a Container for information on assigning media to the container.)

Required Capability: See Capabilities and Permitted Actions

To delete the container information:

1. From the CommCell Browser, right-click the **Containers** icon under **VaultTracker**.

   All the containers are displayed on the right-pane of the CommCell Browser.

2. Right-click the Container that you wish to delete and then click **Delete**.
3. Click **Yes** in the **Confirm** prompt.

   The container is deleted.

ADD MEDIA TO A CONTAINER

Before You Begin

- Add the container information to the system, as described in Add a Container.
- Make sure that the media is marked as exported before adding the media to a container.

Required Capability: See Capabilities and Permitted Actions

T**o add media to a container:**

1. From the CommCell Browser, right-click the **Exported Media** group and then choose **Set Location**.
2. From the Export Media List dialog box, click the media that you wish to move to the container from the **Select Media for which you want to set the location** list. (To select multiple media, press and hold down CTRL or SHIFT keys while clicking.)
3. Select the **Container** option and choose the name of the container in which you wish to move the media from the list.
4. Click OK to save the information.

To add a specific media to a container:

1. From the CommCell Browser, right-click the appropriate media from the **Exported Media** group that you wish to add to a container, and then click **Properties**.
2. From the General tab of **Media Properties** dialog box, select the **Container** option and then select the name of the container to wish you wish to add the media from the list.
3. Click **OK** to save the information.

To add media to a container from a Pending Action:

1. From the CommCell Browser, click the **Actions** icon, under the **VaultTracker**.
   All the VaultTracker pending actions are displayed in the right-pane of the CommCell Browser.
2. Right-click a Pending Action and then click **Set Container**.
3. From the **Set Container** dialog box, select the appropriate container.
4. Click **OK** to save the information.

To add media to a container when the media is marked as Reached Destination:

1. From the CommCell Browser, click the **Actions** icon, under the **VaultTracker**.
   All the VaultTracker jobs with a pending action is displayed in the right-pane of the CommCell Browser.
2. Right-click a Pending Action and then click **Reached Destination**.
3. From the **Set Container** dialog box, select the appropriate container.
4. Click **OK** to save the information.

- You can also automatically create containers and add media associated with VaultTracker Policies as described in Establish Automatic container Generation in a VaultTracker Policy.
- When the capacity of a container has been reached, VaultTracker automatically carries over any remaining media to the next available container defined in the VaultTracker Policy.

Display the Media available in a Container

Required Capability: See Capabilities and Permitted Actions

► To display the media available in a container:

1. From the CommCell Browser, right-click the **Containers** icon under **VaultTracker**.

   All the containers are displayed on the right-pane of the CommCell Browser.

2. Right-click a container and then click **View Media**.
3. The View Media dialog box, displays a list of media available in the container.

Add or Modify the Customer Identification Number

Required Capability: See Capabilities and Permitted Actions

► To add a container:

1. From the CommCell Browser, click the **Iron-Mountain ID** icon under the **VaultTracker** node.
2. Double-click the desired **Customer-Id** on the right pane to add or modify the value.
3. Click **OK** to save the information.

Back To Top

Data Multiplexing

Topics | How To | Support | Related Topics

OVERVIEW

In a typical storage policy configuration, many clients/subclients can point to the same storage policy. Each storage policy copy has one or more streams related to the number of drives in a drive pool. On a particular stream, only one subclient can perform a data protection operation at any one time. The limit for the number of data protection operations that can go to any one stream is one. Therefore, only one data protection operation can be sent to a media/drive at any one time.

This limitation has its disadvantages. Backing up one client/subclient to a single piece of media does not fully utilize the drive's throughput, as the backing up of client data can be much slower than actual speeds of the tape.

In a large enterprise with many clients, many data protection operations may need to be performed within a fixed backup window. This may lead to high hardware requirement costs if the drive or media used for those data protection operations is being under utilized.

To optimally use the high speed tape drives available today, data from several clients/subclients can be multiplexed and written to media.

CHUNK SIZE OF DATA THAT IS MULTIPLEXED

Multiplexed data chunk sizes are determined by the type of data that is being multiplexed; file system data and database data.

- If the first backup is a file system type backup, all other backups joining multiplexing will have a chunk size of 4 GB.
- If the first backup is a database type backup, all other backups joining multiplexing will have a chunk size of 16 GB.

Multiplexed data is aged when all jobs (multiplexed) on a single chunk have met the defined retention rules of their associated storage policy copy. For more information, see Data Aging.

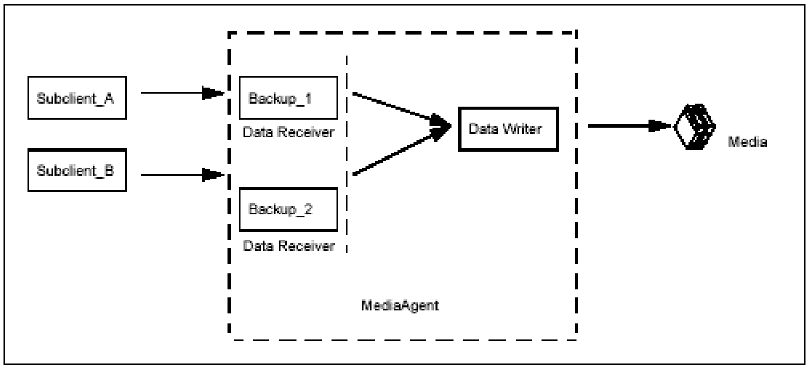
- Data in a storage policy copy enabled for Deduplication can not be multiplexed. Therefore, Data Multiplexing is not supported if the storage policy copy is enabled with Deduplication. However, a SILO copy supports Data Multiplexing even if the storage policy copy is enabled with Deduplication.
- Multiplexed data cannot be copied to a storage policy copy enabled for Deduplication. Therefore, a storage policy copy enabled for Deduplication can not have a direct or indirect source copy enabled for Data Multiplexing.
- An Auxiliary Copy can be configured with Data Multiplexing when the source copy is enabled for Deduplication.

HOW DATA MULTIPLEXING WORKS

During a data protection operation, agent data is transferred to media over a data pipeline. This data is transferred by data movers that read agent data then write the data to the media.

During data multiplexing, many such data movers must read and write data to the same piece of media. To achieve this, these data movers are comprised of two components, data receivers and data writers. During data multiplexing, one data receiver per backup stream reads the data coming through the data pipeline. One data writer per media receives data from multiple data receivers then writes data to the media.

In the sample image that follows, `Subclient_A` and `Subclient_B` are being backed up at the same time and their data is being multiplexed. Multiple data receivers read the data and then one data writer writes the data to a single piece of media.



Configuring for Data Multiplexing

To configure your subclients to use this feature, data multiplexing must be enabled from the `Media` tab of the `Copy Properties` dialog box of the primary copy.

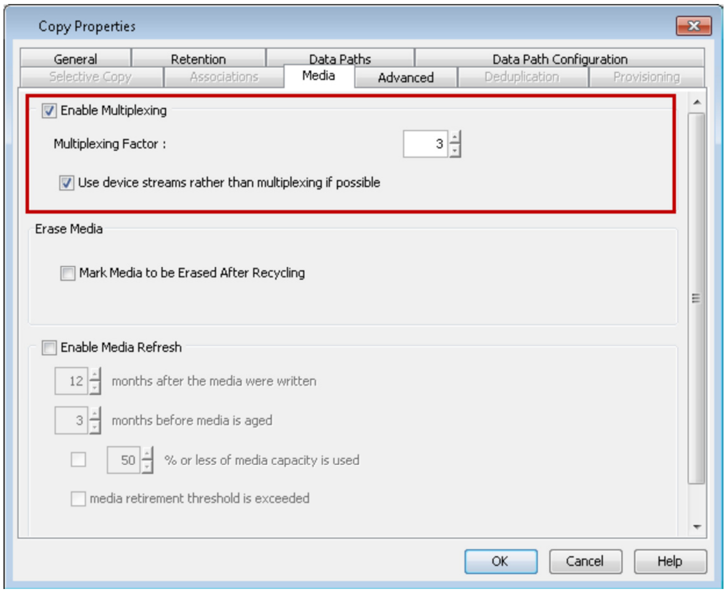
For example, if three subclients of this storage policy are to be backed up in a multiplexed manner, then the multiplexing factor would be set to three.

You can enable multiplexing for the copy as follows:

1. From the CommCell Browser, navigate to **Policies | Storage Policies | *<Storage_Policy>***.
2. Right-click ***<Storage Policy Copy>*** and click **Properties**.
3. Click the **Media** tab.
4. Select the **Enable Multiplexing** check box and select the **Multiplexing Factor**.
5. Select the **Use device streams rather than multiplexing if possible** checkbox.

   The data streams are copied to each available drives first and then fills up the used up drives (spill and fill). If disabled, all the data streams are copied to one drive and once it is filled up, moves to the next drive (fill and spill).

5. Click **OK**.



☑ Enable Multiplexing

Multiplexing Factor : 3

☑ Use device streams rather than multiplexing if possible

Erase Media

☐ Mark Media to be Erased After Recycling

☐ Enable Media Refresh

12 months after the media were written

3 months before media is aged

☐ 50 % or less of media capacity is used

☐ media retirement threshold is exceeded

Determining the Multiplexing Factor

The multiplexing factor should be determined by analyzing your network configuration and by examining your needs for maximizing disk throughput to decrease the total amount of time it takes to protect your data. The multiplexing factor is determined by the following:

- Network card speed
- Network switch speed

- Drive speed

The following examples will help you determine the multiplexing factor. Keep in mind that these are only hypothetical examples.

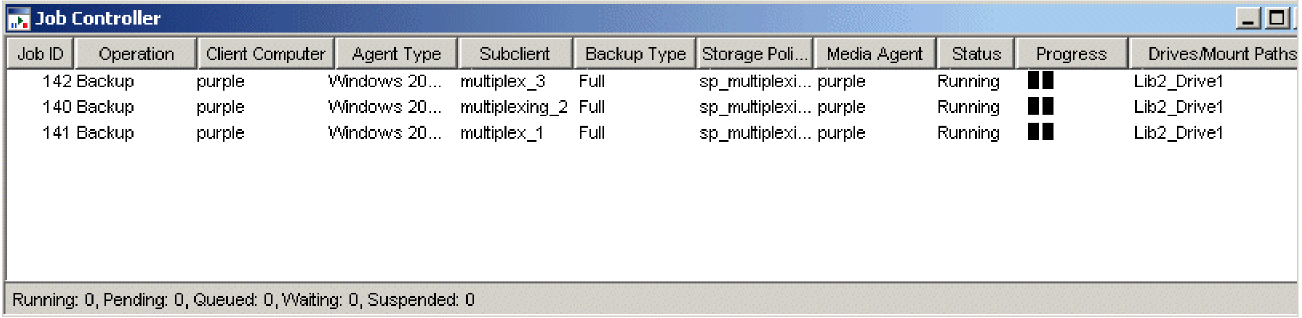
1. Let's analyze a network configuration that involves three clients, without and with multiplexing.
2. What happens when a fourth client is added to the example and the multiplexing factor is set to four.
3. A fifth client is added, and the multiplexing factor is set to five, is this over-multiplexing?
4. If you have over-multiplexed, either set the multiplexing factor lower and multiplex less clients, or add some gigabit Ethernet switches to your network.
5. In another example, client disk speeds are fast and they become slower after multiplexing.

Note that the maximum multiplexing factor that can be set from the CommCell Console is 10 and the system displays a warning message when the multiplexing factor is set to 5 or above.

Perform a Multiplexed Data Protection Operation

Once the multiplexing factor is set on the primary copy of the storage policy whose subclients are to be backed up, all data protection operations of the storage policy can run at the same time, to the same piece of media.

In the sample image that follows, Job IDs `142`, `140`, and `141` are all backing up to `Lib_Drive1`.



Job ID	Operation	Client Computer	Agent Type	Subclient	Backup Type	Storage Poli...	Media Agent	Status	Progress	Drives/Mount Paths
142	Backup	purple	Windows 20...	multiplex_3	Full	sp_multiplexi...	purple	Running	■■	Lib2_Drive1
140	Backup	purple	Windows 20...	multiplexing_2	Full	sp_multiplexi...	purple	Running	■■	Lib2_Drive1
141	Backup	purple	Windows 20...	multiplex_1	Full	sp_multiplexi...	purple	Running	■■	Lib2_Drive1

Running: 0, Pending: 0, Queued: 0, Waiting: 0, Suspended: 0

PERFORM DATA MULTIPLEXING USING A DISK LIBRARY

Data Multiplexing can be performed on a disk library by setting the maximum number of streams on the disk storage policy to a value equal to the number of data protection operations that are to be performed simultaneously. For more information on setting the number of data streams, see Storage Policy Copy Properties.

DE-MULTIPLEXING MULTIPLEXED DATA

De-multiplexing segregates/de-multiplexes the data for selected clients/subclients from the larger list of clients. The software does not require de-multiplexing; however, if you want to de-multiplex the data that you have multiplexed, you can create a subclient-based storage policy copy for each subclient within the original storage policy copy, and then perform an auxiliary copy operation on that copy.

Be sure to adhere to Best Practices when using the data multiplexing feature.

Multiplexing and Data Streams

Data Multiplexing is performed differently based on whether or not you are performing multiple stream data protection operations.

DATA MULTIPLEXING WITH SINGLE STREAM DATA PROTECTION OPERATIONS

In the following example, J_1, J_2, J_3, and J_4 have been run as single stream data protection operations. There are two drives available, D_1, and D_2.

If there is no data multiplexing:

J_1 will use D_1, J_2 will use D_2. J_3, and J_4 will go into a waiting state until J_1 and J_2 have completed.

If data multiplexing was used with a multiplexing factor of two:

J_1 and J_2 will use D_1. J_3 and J_4 will use D_2.

DATA MULTIPLEXING WITH MULTIPLE STREAM DATA PROTECTION OPERATIONS

The following examples illustrate data multiplexing with data protection operations that use multiple streams.

DATA MULTIPLEXING WITH FILE SYSTEM MULTIPLE STREAM DATA PROTECTION OPERATIONS

In the following example, there are two jobs, J_1 and J_2. Each job was run with three streams. There are two drives, D_1 and D_2.

If there is no data multiplexing:

J_1 has three streams, and each stream uses D_1, but they run one after another.

J_2 also has three streams, and each stream uses D_2, and they also run one after another.

If there is data multiplexing with a multiplexing factor of three:

The three streams of J_1 can run concurrently to D_1.

The three streams of J_2 can run concurrently to D_2.

DATA MULTIPLEXING WITH DATABASE MULTI STREAMING

In the following example, a three stream database data protection operation is performed with a multiplexing factor of three. J_1, J_2, and J_3 are database data protection operations, and each used three streams. There are three drives available, D_1, D_2, and D_3.

If there is no data multiplexing:

D_1 - J_1

D_2 - J_1

D_3 - J_1

The second and third job (J_2 and J_3) must wait for the necessary resources.

If there is data multiplexing with a multiplexing factor of three.

The first job (J_1) uses three drives, D_1, D_2, and D_3:

D_1 - J_1

D_2 - J_1

D_3 - J_1

The second and third job (J_2 and J_3) are multiplexed and use the same drives as J_1:

D_1 - J_1, J_2, J_3

D_2 - J_1, J_2, J_3

D_3 - J_1, J_2, J_3

Therefore, J_1, J_2, and J_3 use D_1, D_2, and D_3 in parallel.

DATA MULTIPLEXING WITH MULTI STREAMING FOR ORACLE JOBS

The Oracle *i*DataAgent applies multiplexing rule as any other database *i*DataAgent for multiple jobs. Also, when you have multiplexing enabled for an Oracle job with multiple streams, all the streams of the job can be made to use the available drives sequentially (i.e., fills one drive and then moves to the next) by enabling the **Enable Multiplexing for Oracle** option in the **Job Management** window from the **Control Panel**. For step-by-step instructions on enabling multiplexing for Oracle, see Enable Data Multiplexing.

However, note that this option can be used only for Oracle jobs from the CommCell Console and from third party command line. This can also be used when initiating the job using `qoperation backup` command.

> In the case of on demand Oracle jobs, data multiplexing is enabled by default with/without this parameter. You can disable this feature using the `QB_NO_MULTIPLEX_STREAM` option.

IMPACT OF DATA MULTIPLEXING ON DATA RECOVERY OPERATIONS

The following data recovery operations can be performed on multiplexed data without significant degradation of performance:

- Data recovery operations using CommCell Console
- Data recovery operations using Media Explorer

BEST PRACTICES

It is recommended that you keep the following in mind when performing data multiplexing:

- Use different storage policies for file system and database type data before performing data multiplexing. Therefore, there will not be differences in the chunk sizes of the different types of data.
- If possible use the Restore by Jobs option to restore multiplexed data, especially when restoring large amount of data. This will provide the optimum performance during the restore operation as there are fewer tape rewinds to secure the data.
- It is recommended that you perform data multiplexing for jobs that have similar speeds (i.e. two database jobs), instead of mixing faster jobs (i.e. file systems) with slower jobs (i.e. databases). Mixing faster and slower jobs results in data stored on media that is not uniform.. Hence, data recovery operations of slower clients will have added performance penalty.
- Multiplexing is recommended if you are planning to recover:
  - Individual items, files and folders.
  - Entire computers or databases.
- It is not recommended under following conditions:
  - If you are planning to recover scattered folders as multiplexing will further scatter the data. Also it adds to up to extra tape mounts and rewinding/forwarding on the media.
  - Clients which undergo very frequent restore requests.
- The multiplexing factor is determined based on the ratio of how fast the tape drive is compared to the disk. For example, consider the following ratios:
  - Tape write speed = 80 GB per hour
  - Disk read speed (backup) = 25 GB per hour
  - Tape read speed = 80 GB per hour
  - Disk write speed (restore) = 60 GB per hour

  Tape write speed/disk read speed (backup) = 80/25 = 3.2 GB per hour

  Tape read speed/disk write speed (restore) = 80/60 = 1.33 GB per hour

  It is recommended that the lower of the two ratios as the multiplexing factor if you want no-penalty data recovery operations.

LICENSE REQUIREMENT

This feature requires a Feature License to be available in the CommServe® Server.

Review general license requirements included in License Administration. Also, View All Licenses provides step-by-step instructions on how to view the license information.

Back to Top

Data Multiplexing - How To

Topics | How To | Support | Related Topics

ENABLE DATA MULTIPLEXING

Before You Begin

Data Multiplexing cannot be enabled on a secondary copy, a copy of a disk library, or on a Disaster Recovery Backup storage policy.

Required Capability: Capabilities and Permitted Actions

To enable data multiplexing:

1. From the CommCell Browser, right click the storage policy copy whose storage policy you want to enable data multiplexing, then click **Properties**.
2. From the Media tab of the **Copy Properties** dialog box, select **Enable Multiplexing**.
3. Select the number of subclients whose data will be multiplexed to the same media from the **Multiplexing Factor** list box.
4. Click **OK** to save your changes.

To enable data multiplexing for Oracle jobs:

1. From the CommCell Browser, click **Job Management** from the **Control Panel** window.
2. From the Job Management (General) tab, select **Enable Multiplexing for Oracle**.

3. Click **OK** to save your changes.

Back to Top

Alternate Data Paths (GridStor®)

Topics | How To | Troubleshoot | Examples | Support | Related Topics

Overview

Several data paths can be added to a storage policy copy, to ensure the success of data protection and other operations conducted using the storage policy. A data path is the combination of MediaAgent, Library, Drive Pool and Scratch Pool used by the storage policy copy to perform a data protection operation. Each storage policy copy has a default data path which will be used to perform data protection operations. In addition, you can also define alternate data paths in each of the storage policy copies.

Alternate data paths provide the following advantages:

- Alternate data paths provide the facility to automatically switch over to an alternate data path, when one of the components in the default data path is not available. In addition to ensuring the successful completion of data protection jobs, alternate data paths also utilize available libraries and drives in the event of failure or non-availability of these resources.
- Alternate data paths can be used to minimize media utilization by routing data protection operations from several subclients to the same storage policy and hence the same media, instead of creating several storage policies which in turn utilizes a different media for each subclient.
- In addition, the facility to load balance (round robin) between alternate data paths provides the mechanism to load balance or evenly distribute data protection operations between available resources.

Alternate data paths are supported for both the primary and secondary copies associated with storage policies for all libraries. (See Alternate Data Paths (GridStor) -Support for additional details.) Note, however, that there are several differences between the operations performed using primary and secondary copies with alternate data paths. These are explained in detail in the following sections. Note that within the selected storage policy (and its data paths), the facility to define a subset of the data paths at the subclient level is also provided.

LICENSE REQUIREMENT

This feature does not require any additional license.

Configuring Alternate Data Paths for Primary Copies

The following options are provided while defining alternate data paths on primary copies:

- Facility to automatically configure the data paths for shared libraries.
- Facility to select the alternate data path based on any one of the following:
  - Use alternate data path when resources are busy or offline,
  - Load balance (Round Robin) between available resources, or
  - Use alternate data path to perform LAN-free data protection operations.

    Note that the client and the MediaAgent must be on the same computer, in order to perform a LAN-free operation.

The following sections describes each of these options in detail.

ADDING DATA PATHS TO PRIMARY STORAGE POLICY COPIES

If a storage policy is created during the library configuration process, a default data path is created for the primary copy using the MediaAgent, Library, Drive Pool and default scratch pool combination for drive pools configured within the library. If you create a new storage policy, you must specify a Library, MediaAgent, Drive and Scratch pool combination for the primary copy.

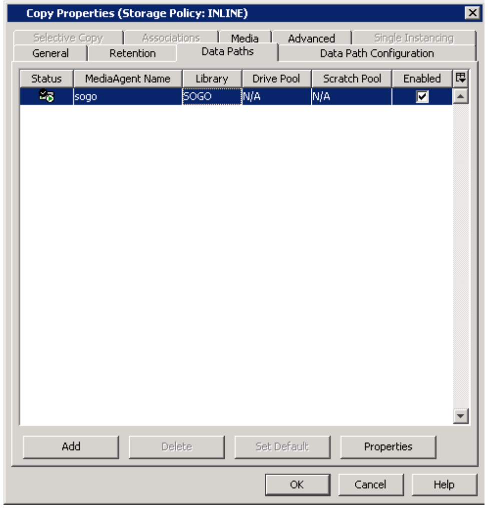
Additional data paths for the primary copy can be defined from the Data Paths tab of the **Copy Properties** dialog box.

See Add a Data Path to a Storage Policy Copy for step-by-step instructions.

The data paths that are available to be added as alternate data paths, depends on the option selected in this dialog box. In addition some of the options may require the index cache to be shared to be accessed as a data path. (These details are explained in the subsequent sections of this document.)

After defining additional data paths, if necessary, you can set any of the data paths as the default data path for the storage policy copy.

See Set a Data Path as the Default Data Path for step-by-step instructions.



Status	MediaAgent Name	Library	Drive Pool	Scratch Pool	Enabled
	sogo	SOGO	N/A	N/A	☑

AUTOMATICALLY ADDING DATA PATHS FOR EXISTING LIBRARIES

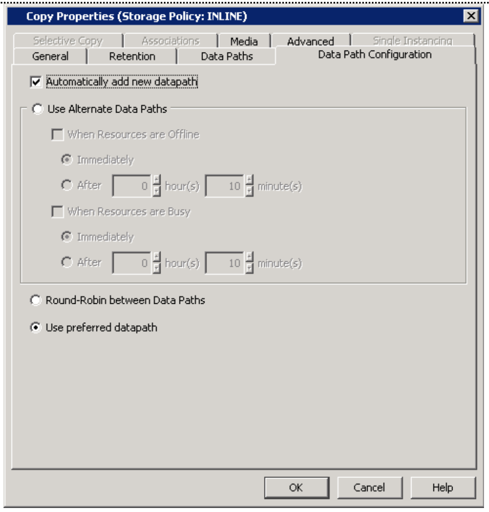
When multiple MediaAgents share the same library (SAN DDS, or direct-attached shared library configurations) the system can automatically add the alternate data paths for each of the storage policies, when this option is enabled. As each of these data paths (MediaAgent, Library, Drive Pool and Scratch Pool) use the same resources, additional index cache configuration is not required. In addition, the criteria for using the alternate data path (described in the following section) must also be specified.

DEFINING THE CRITERIA FOR USING ALTERNATE DATA PATHS

A storage policy can be configured to use an alternate data path using the following criteria:

- When resources are busy or offline - use this option to configure your system to use an alternate data path when resources are busy or offline.
- Load balance between the data paths - use this option to evenly distribute data protection operations amongst drive-pools, thereby not overloading a specific drive-pool.
- LAN preferred data path - use this option to automatically perform LAN-free data protection operations.

Criteria for using alternate data paths can be defined from the Data Path Configuration tab of the **Copy Properties** dialog box. See Select the Criteria for using an Alternate Data Path for step-by-step instructions.



☑ Automatically add new datapath

○ Use Alternate Data Paths

☐ When Resources are Offline

● Immediately

○ After 0 hour(s) 10 minute(s)

☐ When Resources are Busy

● Immediately

○ After 0 hour(s) 10 minute(s)

○ Round-Robin between Data Paths

● Use preferred datapath

WHEN RESOURCES ARE BUSY OR OFFLINE

When this option is selected the system automatically uses an alternate data path when resources are busy or offline.

If the **When resources are offline** option is selected, the storage policy will use an alternate data path when one of the following resources is broken or not available and hence marked as **offline** by the user or by the MediaAgent:

- MediaAgent
- Library
- Master Drive Pool
- Drive Pool
- All the drives in the Drive Pool
- No spare media in the scratch pool associated with the copy

If the **When resources are busy** option is selected, the storage policy will use an alternate data path when all the drives in the library are busy.

In both the above options, you can indicate whether an alternate data path must be used immediately or after the specified amount of time.

The list of data paths that will be available when this option is selected will include the following:

- Data paths associated with MediaAgents that share the library with the default data path. In this case, it is not necessary to share the index cache, but the number of alternate data paths will be limited to the list of MediaAgents that share a library.
- List of MediaAgents that share the index with the MediaAgent associated with the default data path. In this case, as other libraries can be included in the list of data paths several alternate data paths can be added. However, keep in mind that the index cache must be shared.

  See Index Cache for information on the options available for index cache sharing.

ROUND ROBIN BETWEEN DATA PATHS

When this option is selected the system automatically performs load-balancing between the resources (drives in a library or writers in a disk library) available in all the data paths. Keep in mind that the load-balancing is performed at the drive-pool level as opposed to the MediaAgent level.

The following section illustrates the load balancing operation:

If you have defined 5 data paths with 15 resources, and have 25 data protection operations running concurrently at a given time, load balancing would cause the following to occur:

- The first operation will be performed on the default data path.
- The second (and subsequent operations) will be performed in the next data paths, in the order in which it is added in the **Data Paths** tab of the **Copy Properties** dialog box.
- Once the first 5 operations reserves the resources, the sixth operation will be routed to another resource in the default data path, if one is available. The subsequent operations will be routed to the next data path in the order in which it is added in the **Data Paths** tab of the **Copy Properties** dialog box, until all the resources are occupied.
- Once all the resources are used, the system will constantly check for an available resource, and as soon as one is freed the next job in the queue will be automatically routed to use that resource.

All the MediaAgents that share the index cache with the MediaAgent in the default data path will be available as an alternate data path when this option is selected.

See Also:

- Load Balancing Using Spill and Fill

USE PREFERRED DATAPATH

When this option is selected the system automatically performs LAN free backups wherever possible. It is not necessary to share the index cache for this operation and all available MediaAgents will be available as an alternate data path when this option is selected.

SETTING THE NUMBER OF STREAMS FOR ALTERNATE DATA PATHS

When you add or delete an alternate data path, you must reset the number of streams that are defined for the Storage Policy.

The maximum number of streams for a storage policy, with a primary copy that has alternate data paths should be equal to the sum of all unique drives associated with the drive pools and/or the sum of all writers in the mount paths associated with disk libraries in all alternate data paths. Consider the following scenarios, when the maximum number of streams defined is either too many or too little, when you have specified the criteria to immediately use alternate data paths when resources are busy:

- If the maximum number of streams in a Storage Policy is less than the sum of drives/writers in mount paths associated with all the data paths in a primary copy, then all the resources (drives/writers in mount paths) available in the data paths will not be utilized. For example, if the sum of drives/writers in mount paths in all the data paths is 20, and you have specified 10 as the maximum number of streams, at any given time, only 10 jobs would succeed and the remaining jobs would go into the **Waiting** status with the **Job Delay Reason** stating that no resources are available for the job. In such a situation to fully utilize all the available resources, the maximum number of streams should be set to 20.
- If the maximum number of streams in a Storage Policy is more than the sum of drives/writers in mount paths associated with all the data paths in a primary copy, only as many jobs as the total number of available drives will succeed. For example, if the sum of drives/writers in mount paths in all the data paths is 20, and you have specified 30 as the maximum number of streams, at any given time, only 20 jobs would succeed and the remaining jobs would go into the **Waiting** status with the **Job Delay Reason** stating that no resources are available for the job.

JOBS WITH MULTIPLE STREAMS

For multi-stream jobs, the failover will occur only when all the streams have the necessary resources. For example, if you have a job with 5-streams, and if the necessary resources are not available in the default data path, the failover will occur only when the alternate data path has all the necessary resources - MediaAgent, Library and drive pool with 5 drives. This is the case, irrespective of the criteria (When resources are busy, Round Robin between Data Paths options) specified to use alternate data paths.

CONFIGURING ALTERNATE DATA PATHS FOR SECONDARY COPIES

Data paths can be added to secondary copies to enable LAN free Auxiliary Copy operations, so that network resources can be freed wherever possible.

ADDING DATA PATHS TO SECONDARY COPIES

When a secondary copy is created, you must select the default data path for the copy by selecting the MediaAgent, Library, Drive Pool and scratch pool combination. This data path will be used to access the secondary copy when an Auxiliary Copy operation is performed.

However you can add data paths for the secondary copy so that any Auxiliary Copy operations can be performed using a LAN-free data path.

As with the primary copy, additional data paths for the secondary copy can also be defined from the Data Paths tab of the **Copy Properties** dialog box. (See Add a Data Path to a Storage Policy Copy for step-by-step instructions.)

Note that although the **Use preferred datapaths** option is selected, the LAN free Auxiliary Copy operations on the copy is *not* performed until the alternate data paths are selected.

When you add the data path for the secondary copy it is sufficient to add one path per MediaAgent-Library combination. The system automatically uses an available data path to perform LAN free Auxiliary Copy operations. Keep in mind, that when you add data paths in the secondary copies, the system automatically tries to perform a LAN-free read operation. (This is opposed to the primary copies, where the system strives to perform both the read and write operations when the LAN-free option is selected.)

See also:

Although common data paths are defined in primary and secondary copies, another data path is being used for Auxiliary Copy operations.

EXAMPLES

Alternate data paths on Secondary Copies can be used to perform LAN free Auxiliary Copy operations as follows:

- Using disk as primary and a tape/optical library for secondary copies. See Example 1 for more information.
- Using a tape/optical library for both the primary and secondary copies. See Example 2 for more information.

CONFIGURING ALTERNATE DATA PATHS FOR SUBCLIENTS

Each subclient can be configured with a subset of data paths from the data paths available in the storage policy associated with the subclient . The following options are provided while defining the data paths for a subclient:

- Facility to select a subset of data paths from the list of available data paths.
- Facility to assign a priority for the selected data paths.
- If necessary, facility to override the default data path on storage policy and use the other data path from the subset of data paths available for the subclient.

> Note that **Override Datapaths** option is not supported if the subclient is associated with an Incremental Storage Policy.

Note that the data paths and the priority established at the subclient level takes precedence over the data paths defined at the storage policy copy.

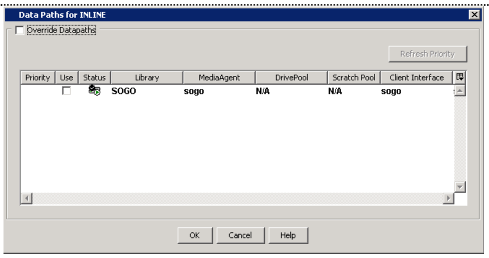
ADDING DATA PATHS TO SUBCLIENTS

By default, the system uses the data path associations defined in the primary copy of the storage policy to perform data protection operations. (This is depicted in the sample image shown on the right. Note that the **Override Datapaths** option is not selected and the default data path is displayed using a bold font-face and a special icon.) If necessary you can perform the following operations:

- Select a subset of the available data paths for the subclient.
- Set a priority for the selected data paths.

See the following procedures for step-by-step instructions:

- Configure Data Paths for Subclients
- Assign Priorities for Subclient Data Paths



Data Paths for INLINE

□ Override Datapaths

Priority	Use	Status	Library	MediaAgent	DrivePool	Scratch Pool	Client Interface
	□		**SOGO**	**sogo**	**N/A**	**N/A**	**sogo**

POINTS TO REMEMBER

Consider the following for configuring data paths at the subclient level:

- Subclient data paths are supported by all agents that require an *i*DataAgent Backup Storage Policy.

  If necessary, different data path subsets can be selected for database agents that use different storage policies for data and log files. (See, Classification of Agents based on Index Usage for a definition of database agents.)
- When a secondary (storage policy) copy is promoted as the primary copy, the data paths defined in the secondary copy is automatically used by the subclient. If necessary, you must establish the default data path and set the priority once the secondary copy is promoted.
- When a data path is deleted from the storage policy (or a library is deconfigured) the data path is automatically removed from the subclient.
- Subclient data paths are not supported by Subclient Policies.
- Subclient data paths cannot be configured using the Command Line interface.
- In the case of Incremental Storage Policies, which uses two different storage policy copies for full and non-full backups, different data path subsets can be

selected for full or non-full backups using the same or a different storage policy. In such a situation, make sure that the selected data paths share the index.

EXAMPLES

The subclient data paths can be used effectively in the following situations:

- To configure subclients to use certain data paths, and minimize media utilization. See Example 1 for information on how this works.
- Restrict some subclients to use only a subset of data paths and at the same time reduce media utilization. See Example 2 for information on how this works.

DATA PROTECTION OPERATIONS USING ALTERNATE DATA PATHS

When a data protection operation is initiated, the storage policy copy attempts to write the data using the default data path. If the default data path is not available, an alternate data path is automatically used to perform the data protection operation. If more than one alternate data path is defined, the first data path listed in the Data Paths tab of the **Copy Properties** dialog box is selected, followed by the second and so on until a data path is available.

MEDIA USAGE

If both the default and alternate data paths are configured to use the same library, as a result of a shared library configuration (configured as a SAN DDS library or direct-attached shared library) the MediaAgent will automatically use the appropriate **Assigned** media for the data protection operation.

If the default and alternate data paths are configured to use different libraries, the MediaAgent, marks the previously used **Assigned** media as **Appendable** and uses a new media from the library associated with the alternate data path.

Such **Appendable** media can be re-used in the library by enabling the **Use Appendable Media** option in the Library Properties dialog box associated with the library.

DATA RECOVERY OPERATIONS USING ALTERNATE DATA PATHS

Data can be restored/recovered from any compatible library and drive type in the CommCell.

WHEN MEDIA IS AVAILABLE IN A LIBRARY

When a Data Recovery operation is initiated, and if the media is not exported, the software attempts to restore/recover data using the appropriate data path associated with that library, instead of the default data path in the following order:

- The first priority is provided to the path which results in LAN-free restore/recover to the client computer from which the restore/recover operation was initiated. LAN-free operation is possible only when the client initiating the restore/recover operation and MediaAgent are on the same computer.
- If the LAN-free operation is not possible, then the Data Recovery operation attempts to restore/recover data using the default data path.
- If the appropriate media is not available in all these data paths, the software automatically identifies the media in which the data resides and performs the restore/recover operation from that library.

WHEN MEDIA IS EXPORTED

When a Data Recovery operation is initiated, and if the media is exported, the software will prompt you to import the media in the appropriate MediaAgent computer. This is done as follows:

If a LAN-free restore/recover is possible, the restore/recover operation would prompt you to import the media in the appropriate library from which the LAN-free restore is possible. (LAN-free restore will be possible only when the client initiating the restore/recover operation and MediaAgent are on the same computer.)

If the LAN-free restore/recover operation is not possible, then the operation would prompt you to import the media in the library which was last used to write to the media.

If the resources in that library are offline, the restore/recover operation would prompt you to import the media in the library associated with the default data path.

If the resources associated with the default data path are offline, then the restore/recover operation identifies a library from an alternate data path which are assigned in the data path list, to import the media.

See Also:

- Restore From Anywhere

IMPORTANT CONSIDERATIONS

Consider the following information when using alternate data paths:

GENERAL CONSIDERATIONS

- Job Preemption is supported on Default/LAN-free backups (i.e., if GridStor is configured for User Preferred Datapath). It is not supported for the jobs that are run using data paths with the Round Robin configuration.
- Change Data Path (right-click option) should not be performed on Storage Policies with Storage Policy Copies that have Alternate Data Paths (GridStor). If Change Data Path is performed on such a setup, data recovery operations can be performed from the media. However, subsequent data protection operations will not re-use the migrated media.

CLUSTERED ENVIRONMENT

- On clustered computers the system automatically performs LAN free operations for Agents installed on the virtual machines with the storage policy copy (attached to the subclient) pointing to the MediaAgent on the physical node. Consider the following example:

  A file system *i*DataAgent is installed on Virtual Machine (VM1) and can be controlled by Node 1 or Node 2 at any given time.

  The subclient (subclient1) associated with this file system *i*DataAgent on VM1 points to a Storage Policy Copy (SP1) which in turn uses the following data paths:

  - default data path using MediaAgent (Node1) and Library 1
  - alternate data path MediaAgent (Node2) and Library 1

  When a backup is run on subclient1, the system automatically figures out the node controlling VM1 and will use the appropriate MediaAgent. For example if VM1 is controlled by Node 2 at the time of the backup, the system automatically uses the MediaAgent on Node2 to perform the LAN free backup.

This capability allows you to install the MediaAgent on the physical node of a cluster. (Instead of multiple instances if installed in the cluster group.) However you will need GridStor® to provide failover capabilities.

CONSIDERATIONS FOR NAS ATTACHED LIBRARIES

- Data paths for NAS attached libraries can only be added if the MediaAgent used in that data path also has the File System *i*DataAgent installed on that computer. This is applicable only for Windows MediaAgents.
- For NAS environments, refer to Storage Policy Considerations for additional information.

CONSIDERATIONS FOR BACKING UP THE MICROSOFT VIRTUAL SERVER

- If the MediaAgent software is installed in the cluster server, configure a disk library to backup the data.
- If you wish to configure a tape/optical library, install the MediaAgent software on the physical computer.

  Add a data path which uses this MediaAgent, Library, Drive Pool and Scratch Pool combination to the Storage Policy used to backup the cluster server. (See Add a Data Path to a Storage Policy Copy for step-by-step instructions.)

  Assign this as a high priority data path in the subclient(s) used to backup the cluster server. (See Assign Priorities for Subclient Data Paths for step-by-step instructions.)

CONFIGURING ROUND ROBIN OF HBA CARDS

When the devices are configured from different HBA cards on the same host as distinct drive pools, each of these drive pools can be added as data paths on the storage policy. For LAN storage policies, these data paths can be added as additional data paths with the **Round-Robin between Data Paths** option enabled. This will automatically round robin the data protection jobs between these HBA cards.

For LAN free Storage Policies, the additional LAN free data paths for the secondary HBA cards can be added as data paths and the software will automatically pick the least used LAN free data path.

(See Configuring Dual Host Bus Adaptors (HBA) for information on configuring HBA cards.)

ROUND ROBIN WITH MULTIPLEXING

When a storage policy is configured for multiplexing and contains data paths to be used in round-robin fashion, then the round-robin option is completely utilized before using multiplexing.

For example, consider a storage policy with 3 data paths configured in the round robin mode and multiplexing set to 2. If 4 backup jobs kick off simultaneously, then the three available data paths are utilized first and multiplexing is applied for the fourth job only.

BEST PRACTICES

Consider the following information and recommendations, while creating and using alternate data paths:

- For LAN-free clients do not enable the **When Resources are Busy** option to choose an alternate data path. This will ensure LAN free operations, wherever possible.

- It is not necessary to share the index on MediaAgents with LAN-free data paths. However, even if one additional alternate data path on the LAN is added to the storage policy, you must share the index for all the MediaAgents in the data path list.
- Create and use less number of storage policies, as large number of storage policies will result in the fragmentation of data on media. Consider the following:
  - Control data retention by creating copies within the Storage Policies. (As opposed to creating many storage policies with different retention periods.)
  - Consolidate each Client's data by creating Subclient-Based Storage Policy Copies.
- Before you deconfigure a library, verify and ensure that none of the Storage Policy Copy's default data path points to the library. (See View the Storage Policies Accessing a Library for step-by-step instructions on how to view the storage policies associated with a library.) If necessary, set an alternate data path as the default data path before deconfiguring the library.

  If you have a storage policy copy with no default data path, use **Change Data Path** option to migrate the storage policy to point to another data path. See Change Data Path for more information.
- NAS Load-Balancing - in addition to the resource load balancing that the Alternate Data Paths feature provides, NAS can be configured to load balance the processing tasks associated with backup, restore, and auxiliary copy jobs, which normally run on a single client machine, to spread the processing among different MediaAgent.

Back to Top

Alternate Data Paths (GridStor) - How To

Topics | How To | Troubleshoot | Examples | Support | Related Topics

CONFIGURE MULTIPLE DATA PATHS FOR A STORAGE POLICY COPY

Required Capability: See Capabilities and Permitted Actions

To configure multiple data paths for a storage policy copy:

1. Select the criteria under which a storage policy copy must use an alternate data path, as described in Select the Criteria for using an Alternate Data Path.
2. Depending on the criteria selected for using an alternate data path, you may have to share the indexes.
3. Add the data paths to storage policy copies for which you wish to add multiple data paths, as described in Add a Data Path to a Storage Policy Copy.

The storage policy copy will automatically switch to an alternate data path, when the preferred data path is either offline or busy, as established in the criteria for using an alternate data path.

SELECT THE CRITERIA FOR USING AN ALTERNATE DATA PATH

Required Capability: See Capabilities and Permitted Actions

To select the criteria for using an alternate data path for a storage policy copy:

1. From the CommCell Browser, right-click the storage policy copy for which you select the criteria for using an alternate data path, then click **Properties**.
2. Click the Data Path configuration tab.
3. Select the **Automatically add datapaths for existing library** option, if you are using shared libraries.
4. Choose from the following options:

Choose the **Use Alternate Data Paths only when** option to indicate that alternate data paths must be used only when resources are busy and/or resources are offline. If you wish to choose this option, and wish to use some or all available resources in the CommCell, you must first share the index cache.

- Select the **When Resources are Offline** checkbox, to indicate that the storage policy copy must use an alternate data path, when resources are offline.

  Resources are MediaAgent, Library, Master Drive Pool, Drive Pool, Drives in the drive pool and spare media in the scratch pool associated with this data path.

  - Select Immediately to use an alternate data path at once, when resources are offline.
  - Select After and type the minimum number of hours and minutes after which an alternate data path must be used when resources are offline
- Select the **When Resources are Busy** checkbox, to indicate that the storage policy copy must use an alternate data path when resources are busy.

  Resources are all the drives in the library attached to the preferred MediaAgent.

  - Select **Immediately** to use an alternate data path at once, when resources are busy.
  - Select **After** and type the number of hours and minutes after which an alternate data path must be used, when resources are busy.

Choose the **Round-Robin between Data Paths** option to automatically fail over between all the available data paths. If you wish to choose this option, you must first share the index cache.

Choose the **Use preferred datapath** option to automatically perform LAN-free backups, wherever possible.

5. You can now add the appropriate data paths as described in Add a Data Path to a Storage Policy Copy.

ADD A DATA PATH TO A STORAGE POLICY COPY

Required Capability: See Capabilities and Permitted Actions

To add a data path to a storage policy copy:

1. From the CommCell Browser, right-click the storage policy copy for which you wish to add the data paths, then click **Properties**.
2. Click the Data Paths tab. Note that depending on the criteria selected for using an alternate data path, you may have to share the indexes.
3. Click **Add**.
4. From the Copy Data Path Candidates dialog box, select the data path candidates that you wish to add.

   You can select multiple candidates by holding down the CTRL key and clicking on each of the data path candidates that you wish to select.
5. Click **Add**.
6. Click **OK.**
7. Click **OK** in the **Data Paths** tab to save the information.

DELETE A DATA PATH FROM A STORAGE POLICY COPY

Required Capability: See Capabilities and Permitted Actions

To delete a data path from a storage policy copy:

1. From the CommCell Browser, right-click the storage policy copy for which you wish to delete a data path, then click **Properties**.
2. Click the Data Paths tab.
3. Click the data path you wish to delete from the list.
4. Click **Delete**. The data path is deleted.
5. Click **OK** to save the information.

   - You cannot delete a data path that is set as the default data path.
   - You can delete a data path when the associated storage policy is reserved for data protection operations.

SET A DATA PATH AS THE DEFAULT DATA PATH

Required Capability: See Capabilities and Permitted Actions

To set a data path as the default data path from a storage policy copy:

1. From the CommCell Browser, right-click the storage policy copy for which you wish to set as the preferred data path, then click **Properties**.
2. Click the Data Paths tab.
3. Click the data path you wish to set as the preferred data path from the list.
4. Click **Set Default**.

   The data path is set as the default data path. Notice the tick mark in the icon displayed in the **Status** column.
5. Click **OK** to save the information.

View Data Paths Associated with a Subclient

Required Capability: See Capabilities and Permitted Actions

To view data paths:

1. From the CommCell Browser, right-click the subclient whose data paths you want to view, then click **Properties** from the shortcut menu.
2. Click the Storage Device tab of the Subclient Properties dialog box.
3. From the **Data [or Logs] Storage Policy** tab, click **Show Data Paths** to view the data paths used by the subclient to access the storage media for data protection operations. Click **Close** to exit the Data Paths dialog box.
4. Click **OK** to exit the Subclient Properties Storage Device tab.

Configure Data Paths for Subclients

Required Capability: See Capabilities and Permitted Actions

To configure data paths for subclients:

1. From the CommCell Browser, right-click the subclient for which you wish to create the data paths, and then click **Properties**.
2. Click the Storage Device tab.
3. Click **Data Paths**.
4. From the Data Paths for <*Storage Policy Name*> dialog box, select the **Override DataPaths** option. This will allow you to define the necessary data paths at the subclient level.
5. From the list of data paths displayed in the bottom pane, select the **Use** option to choose a data path for the subclient.
6. If necessary assign a priority as described in Assign Priorities for Subclient Data Paths.
7. Click **OK** to save the changes.

The selected data paths will be used by the subclient for subsequent data protection operations.

Assign Priorities for Subclient Data Paths

Required Capability: See Capabilities and Permitted Actions

To assign priorities for subclient data paths:

1. Follow the steps described in Configure Data Paths for Subclients.
2. From the Data Paths for <*Storage Policy Name*> dialog box, after selecting the data paths for the subclient by clicking the **Use** option, click **Priority** and type a number as priority.
3. If necessary, click the **Refresh Priority** button to sort the display based on the established priority.
4. Click **OK** to save the changes.

The data path with the smallest number will be established as a high priority data path, while data paths with bigger numbers will be established as low priority data paths.

Managing Media in a Library

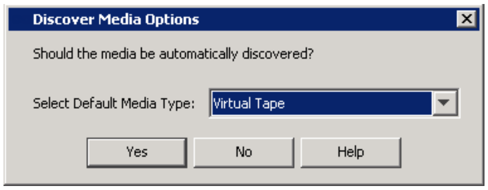
Topics | How To | Related Topics

OVERVIEW

Several features to automate the process of managing media within the library are provided. The following sections provide a detailed discussion on each of these options.

You can automate the media discovery process in the library using one of the following methods:

When you configure a library, select the default media type and then click **Yes** in the **Discover Media Options** dialog box to automatically discover the media in the library.

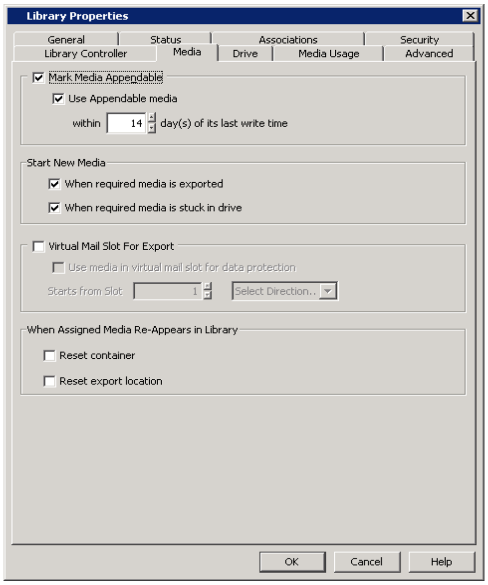


Discover Media Options

Should the media be automatically discovered?

Select Default Media Type: Virtual Tape

If you have already configured the library and have not enabled the automatic media discovery during configuration, you can enable the **Auto Discover Media** option in the **Media** tab of the **Library Properties** dialog box.



Library Properties

☑ Mark Media Appendable
☑ Use Appendable media
within 14 day(s) of its last write time

Start New Media
☑ When required media is exported
☑ When required media is stuck in drive

☐ Virtual Mail Slot For Export
☐ Use media in virtual mail slot for data protection
Starts from Slot 1 Select Direction..

When Assigned Media Re-Appears in Library
☐ Reset container
☐ Reset export location

Once the automatic media discovery process is enabled you can use the following mechanisms to manage media:

- Manage Media Using Barcode Patterns
- Manage Media Using Priority Schemes
- Manage Cleaning Media in the Library

The following sections describe each of these options in detail.

MANAGE MEDIA USING BARCODE PATTERNS

This automated method of distributing media can be used when you have different barcode schemes or specific barcode ranges associated with specific purposes in the library. For example:

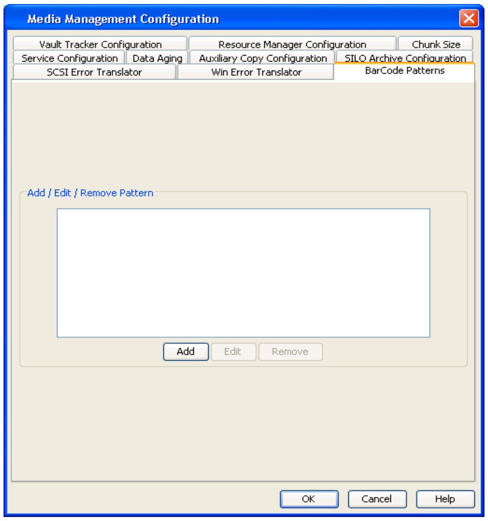
- When you have a library with different drive types, you could have specific barcodes for media associated with each drive type. We highly recommend this method when you multiple drive types in the library. This will help you to easily manage and administer the media in the library.

- When you have media that are not used by the MediaAgents in this CommCell (referred to as Foreign media in the software) stored in the library and use VaultTracker to manage the media movement of such media, you can use specific barcode patterns or ranges for foreign media.
- If you already manage media using barcode patterns, you can use this method to automate the process.

SETTING UP MEDIA MANAGEMENT USING BARCODE PATTERNS

When you use one or more standard barcode pattern(s) in the libraries in the CommCell, you can define from the **BarCode Patterns** tab in the **Media Management Configuration** dialog box. This dialog box is accessible from the CommCell Console Control Panel.(See Add/Modify Barcode Patterns for Media in a CommCell for step-by-step instructions.)

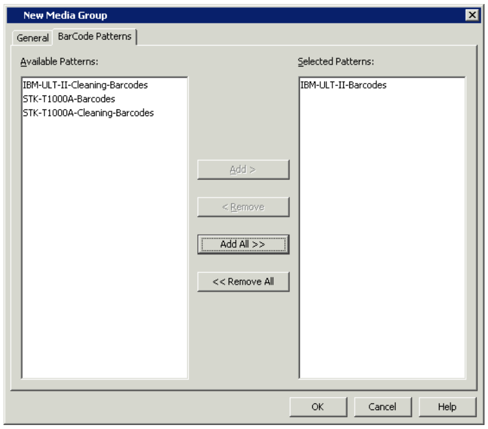
(You can add, modify and if necessary, delete existing barcode patterns in the CommCell from this dialog box.)


Media Management Configuration
Vault Tracker Configuration
Resource Manager Configuration
Chunk Size
Service Configuration
Data Aging
Auxiliary Copy Configuration
SILO Archive Configuration
SCSI Error Translator
Win Error Translator
BarCode Patterns
Add / Edit / Remove Pattern
Add
Edit
Remove
OK
Cancel
Help

Once the specific barcode patterns are defined, you can associate the barcode patterns for the following Media Groups:

- Default and <user-defined> scratch pools
- Cleaning Media group
- Foreign Media group

See Associate (or Disassociate) Barcode Patterns to a Media Group for step-by-step instructions.



Available Patterns:
IBM-ULT-II-Cleaning-Barcodes
STK-T1000A-Barcodes
STK-T1000A-Cleaning-Barcodes

Selected Patterns:
IBM-ULT-II-Barcodes

Once this barcode pattern scheme is setup in the library, the system will automatically move the existing media in the library to the appropriate media groups. Media which do not belong to an existing pattern will be moved to the default scratch pool.

Similarly whenever media is imported or recycled, the system will automatically move the media to the appropriate media group.

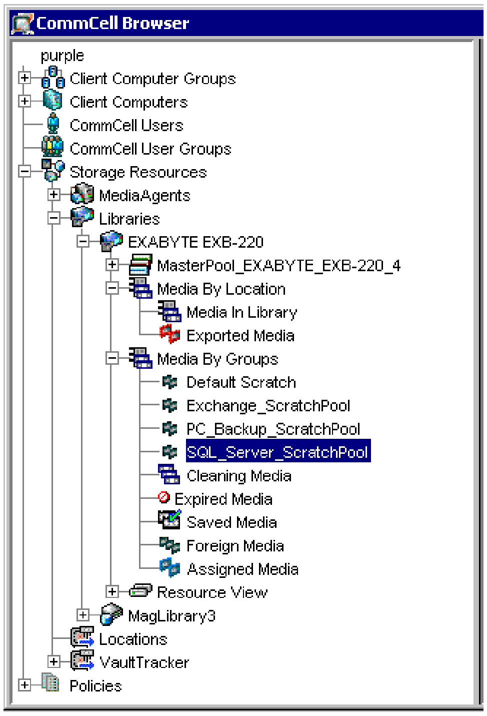
Note that at any point you can also manually move the media between the media groups, if necessary.

MANAGE MEDIA USING PRIORITY SCHEMES

This automated method of distributing media can be used to ensure that high-priority operations always have the necessary media. For example, assume that you regularly back up both a file server with a large database containing mission-critical data and a number of user PCs. You may want to prevent situations in which data secured from less important user PCs use up all available media, causing vital data protection operations on file server to fail. You can do this by creating a scratch pool specifically for the storage policy copies that conduct data protection operations on file servers. Once the scratch pool is setup you can setup a priority scheme for media as explained in the following section.

SETTING UP MEDIA MANAGEMENT USING PRIORITY SCHEMES

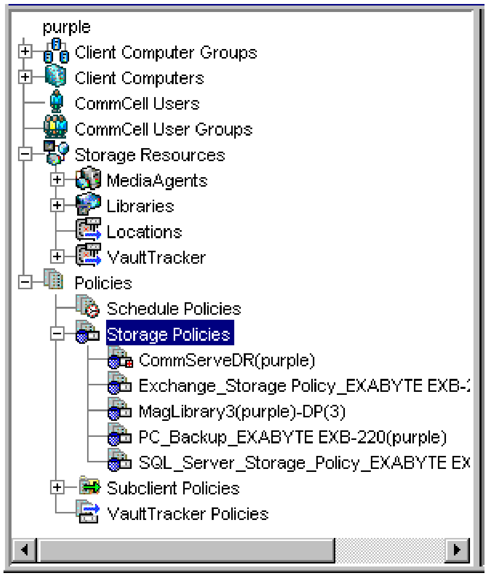
Create appropriate scratch pools for each category of data protection operation. For example, in the sample image appropriate scratch pools have been created for the each of the major data protection requirements.



CommCell Browser

- purple
  - Client Computer Groups
  - Client Computers
  - CommCell Users
  - CommCell User Groups
  - Storage Resources
    - MediaAgents
    - Libraries
      - EXABYTE EXB-220
        - MasterPool_EXABYTE_EXB-220_4
        - Media By Location
          - Media In Library
          - Exported Media
        - Media By Groups
          - Default Scratch
          - Exchange_ScratchPool
          - PC_Backup_ScratchPool
          - SQL_Server_ScratchPool
          - Cleaning Media
          - Expired Media
          - Saved Media
          - Foreign Media
          - Assigned Media
        - Resource View
      - MagLibrary3
    - Locations
    - VaultTracker
  - Policies

Associate each scratch pool to an appropriate storage policy. For example, in the sample image appropriate storage policies have been created for the each of the major data protection requirements.



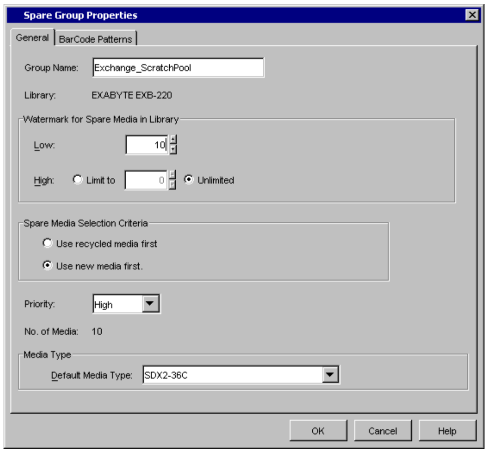
- purple
  - Client Computer Groups
  - Client Computers
  - CommCell Users
  - CommCell User Groups
  - Storage Resources
    - MediaAgents
    - Libraries
    - Locations
    - VaultTracker
  - Policies
    - Schedule Policies
    - Storage Policies
      - CommServeDR(purple)
      - Exchange_Storage Policy_EXABYTE EXB-2
      - MagLibrary3(purple)-DP(3)
      - PC_Backup_EXABYTE EXB-220(purple)
      - SQL_Server_Storage_Policy_EXABYTE EX
    - Subclient Policies
    - VaultTracker Policies

Create the priority scheme as follows:

- Establish a Watermark for each of the media pools.
- Indicate whether new media or recycled media should be used first.
- Establish the Priority for the media group.

For example, in the sample image, since the scratch pool is associated with mission critical jobs, the low watermark is set to 10 and the priority has been set as High. This will ensure the following:

- That a minimum of 10 media will always be available in the scratch pool. (When the minimum falls below the established watermark, the system generates an Event message and also generates an alert, if configured.)
- When new media is imported, or when existing media is recycled, the system will always assign media to media groups priority set to high until the Watermark is reached, before assigning them to Medium and Low priority media groups.



Group Name: Exchange_ScratchPool

Library: EXABYTE EXB-220

Watermark for Spare Media in Library

Low: 10

High: ○ Limit to 0 ● Unlimited

Spare Media Selection Criteria

○ Use recycled media first

● Use new media first.

Priority: High

No. of Media: 10

Media Type

Default Media Type: SDX2-36C

For Spare Media Selection Criteria, the system chooses the media as follows:

- If the **Use recycled media first** option is chosen, the system will select a media based on how many times the media was reused - the media with the highest value will be selected. For example, if you have 2 media, one media that has been re-used 3 times and another 2 times, the media which has been re-used 3 times will be selected first. If more than one media has the same value, the media which was discovered the earliest will be used from the media that has the same values.
- If the **Use new media first** option is chosen, the system will select the media based on the discovery time - the media that was discovered the earliest will be selected. If there are no unused media, then the system uses the reverse criteria described above - the media with the minimum number of reuses is selected and if more than one media has the same value, between the media that has the same value, the media with the most recent discovery time is selected.

Keep in mind that excess media (beyond the watermark established in each media group) will be moved to the default scratch pool.

Also note that at any point you can also manually move the media between the media groups, if necessary.

MANAGE CLEANING MEDIA IN THE LIBRARY

Most cleaning media have a standard barcode pattern. For example, many of the cleaning media have the alphabets "CL" in the beginning. Such specific barcode patterns on cleaning media can be used to discover cleaning media and automatically move them to the **Cleaning Media Pool**, when the automatic media discovery option is enabled in a library.

Cleaning media can also be automatically moved to the cleaning media pool as described in Manage Media Using Barcode Patterns. Also, read the information in Cleaning Media for complete information on managing cleaning media.

Managing Media in a Library - How To

Topics | How To | Related Topics

Add/Modify Barcode Patterns for Media in a CommCell

Delete Barcode Patterns for Cleaning Media in a CommCell

Associate (or Disassociate) Barcode Patterns to a Media Group

ADD/MODIFY BARCODE PATTERNS FOR MEDIA IN A COMMCELL

Required Capability: See Capabilities and Permitted Actions

To add/modify barcode patterns for media in a CommCell:

1. From the **Tools** menu in the CommCell Console, click **Control Panel.**
2. Double-click **Media Management Configuration**.
3. Click the BarCode Patterns tab.
4. Click **Add**.

or

Click the pattern and then click **Edit** to modify an existing pattern.

5. From the BarCode Pattern dialog box establish a barcode pattern using the various options provided.
6. Click **OK**. The pattern is displayed in the **Add / Edit / Remove Pattern** box.
7. Click **OK** to save the changes.

DELETE BARCODE PATTERNS FOR MEDIA IN A COMMCELL

Required Capability: See Capabilities and Permitted Actions

BEFORE YOU BEGIN

- Make sure that the barcode pattern that you wish to delete are not associated with a barcode pattern defined for a library. For more information, see Associate (or Disassociate) Barcode Patterns to a Media Group.

▶ To delete barcode patterns for media in a CommCell:

1. From the **Tools** menu in the CommCell Console, click **Control Panel.**
2. Double-click **Media Management Configuration**.
3. Click the BarCode Patterns tab.
4. Click the barcode that you wish to delete from the **Add / Edit / Remove Pattern** box and then click **Remove**.
5. The pattern is removed from the **Add / Edit / Remove Pattern**.
6. Click **OK** to save the changes.

ASSOCIATE (OR DISASSOCIATE) BARCODE PATTERNS TO A MEDIA GROUP

Required Capability: See Capabilities and Permitted Actions

▶ To associate (or disassociate) barcode patterns to a Media Group:

1. From the CommCell Browser, right-click the appropriate media group (**Default** or ***<user-defined>* scratch pools**, **Cleaning Media**, or **Foreign Media** group) and then click **Properties**.
2. Click the Barcode Patterns tab.
3. To associate a barcode, click the barcode you wish to associate from the **Available Patterns** list and then click **Add**.

   If the **Available Patterns** list does not contain the specific barcode pattern used in the library, add the pattern as described in Add Barcode Patterns for Media in a CommCell.
4. To disassociate a barcode, click the barcode you wish to disassociate from the **Selected Patterns** list and then click **Remove**.
5. Click **OK** to save the changes.

The selected barcodes will be used to identify media and automatically move them to the appropriate Media pool, if the **Enable Auto-Discover Media into default scratch pool** option is enabled in the Library Properties (Media) tab.

Recall Media

Topics | How To | How Do I | Related Topics

OVERVIEW

The Recall Media feature provides the facility to temporarily bring media back from an export location for a specific operation and return the media to the export location when the operation is complete. This capability is useful if you have exported media to another location with the intention of keeping the media at the export location for an established period of time, but need to bring the media back from the export location for a specific purpose (such as a data recovery operation) prior to the original return date.

When a media is recalled, a new pending action is automatically created in the **VaultTracker | Actions** node in the CommCell Console, which you can track or modify as you would any other pending action.

Once the recall action has been initiated, the media is returned to the library of your choice where it will remain either indefinitely or for a specific period of time, depending on the option you selected. If a container was created for the media using VaultTracker Enterprise, the media will be recalled using the original container. While returned to the source location, the media will automatically be protected from any erroneous export operations, accidental overwrites, etc., for the duration of the recall operation. When the recall operation is complete, the media will be sent back to the export location (along with the original container, if applicable) using the original tracking policy.

HOW TO RECALL MEDIA

For step-by-step instructions on recalling media, see the following:

- Recall Media using List Media (Media Prediction)
- Recall Media using the Resource View

ALERTS CONFIGURATION

Alerts allow you to send notifications related to recall media operations. Alerts can be configured by creating a Library Management alert and selecting **Media Recalled** as the notification criteria. For a detailed explanation of Alerts, see Alerts and Monitoring.

See Configure Global Alerts for step-by-step instructions on creating alerts.

POINTS TO REMEMBER WHEN RECALLING MEDIA

- If you choose the **Infinite** option for the **Expiration Date**, the media will remain in the **Recall** state until you manually right-click the action and select **Recall Done**. The media will then be marked **Available for Export**.
- If you choose a specific date and time for the **Expiration Date**, ensure that the media will no longer be needed by the date specified as the media will be marked **Available for Export** on the expiration date.
- By default, the MediaAgent retains the container and export location associated with the Media. These associations are viewable from the Media Properties - General tab. If necessary, you can enable a global option in the library from the Library Properties -Media tab, to automatically remove these associations when the media is brought back in to the library.

LICENSE REQUIREMENTS

This feature requires a VaultTracker Enterprise license.

For information on license requirements, see VaultTracker® Licenses in License Administration.

Recall Media - How To

Topics | How To | How Do I | Related Topics

Recall Media using List Media (Media Prediction)

Recall Media using the Resource View

RECALL MEDIA USING LIST MEDIA (MEDIA PREDICTION)

Required Capability: See Capabilities and Permitted Actions

► To recall media using List Media (Media Prediction):

1. From the CommCell Browser, right-click the subclient associated with the media you wish to recall and click **List Media**.

   Note that you can use the **Specify Browse Time** and **Exclude Data Before** options to list media between a specified date and time range.
2. From the List Media dialog box, select the media you wish to recall and click **Recall Media**.

   The **Recall Media** dialog box appears.
3. From the **General** tab, select the following:
   - The time until which the media would be retained in the library for read operations.
   - A reason for recalling the media.
4. From the **Destination** tab, configure the following destination options:
   - Click the **Track Transit** option and select the transit location from the list, to track the transit information.
   - Select the desired **Destination**.
   - If desired, select the **Move Media to Overwrite Protection Pool** option along with the desired pool to which the media will be moved.
   - Select **Acknowledge the action as Reached Destination automatically** if desired.

     Note that this option is not available if **Indefinite** is selected in the **General** tab.
5. Click **OK**.

The recall media action is now initiated and viewable in the **VaultTracker | Actions** node of the CommCell Console.

RECALL MEDIA USING THE RESOURCE VIEW

Required Capability: See Capabilities and Permitted Actions

► To recall media using the Resource View:

1. From the CommCell Browser, navigate to the media you wish to recall:
   - Expand the **Storage Resources | Libraries** nodes.
   - Select the library from which the media you wish to recall was originally exported.
   - Expand the **Media by Location** node.
   - Select **Exported Media**. The exported media you wish to recall will appear in the **Resource View**.
2. Right-click on the media you wish to recall and select **Recall Media**.

   The **Recall Media** dialog box appears.
3. From the **General** tab, select the following:
   - The amount of time the media would be retained in the library for read operations.
   - The reason for recalling the media.
4. From the **Destination** tab, configure the following destination options:
   - Click the **Track Transit** option and select the transit location from the list, to track the transit information.
   - Select the desired **Destination**.
   - If desired, select **Move Media to Overwrite Protection Pool** along with the desired pool to which the media will be moved.
   - If desired, select **Acknowledge the action as Reached Destination automatically**.

     Note that this option is not available if **Indefinite** is selected in the **General** tab.

5. Click **OK**.

The recall media action is now initiated and viewable in the **VaultTracker | Actions** node of the CommCell Console.

Orphaned Media

OVERVIEW

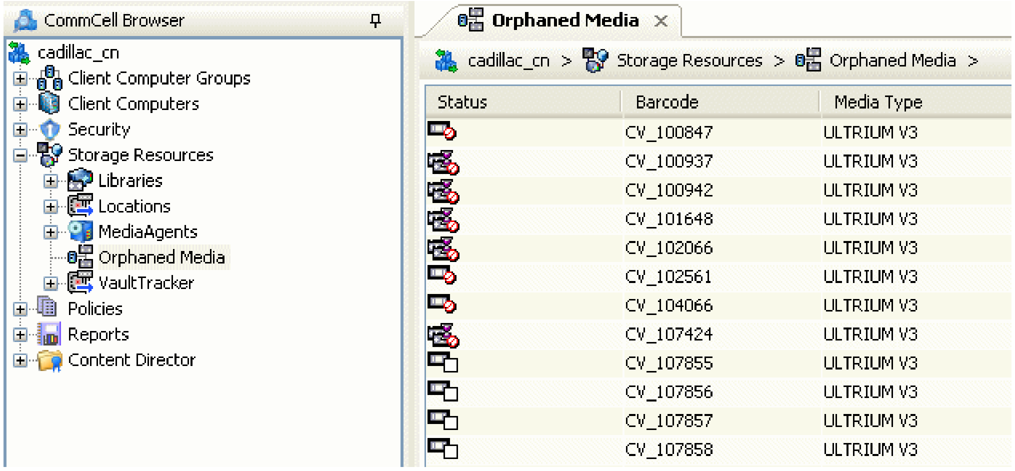
Orphaned media is a logical repository of all the assigned media which does not have any associated libraries. The following sections describe media operations that can be performed for the Orphaned Media.

OPERATIONS

VIEW ORPHANED MEDIA

To view all the Orphaned Media:

In the Commcell Browser, click **Storage Resources** and click **Orphaned Media**.



Status	Barcode	Media Type
	CV_100847	ULTRIUM V3
	CV_100937	ULTRIUM V3
	CV_100942	ULTRIUM V3
	CV_101648	ULTRIUM V3
	CV_102066	ULTRIUM V3
	CV_102561	ULTRIUM V3
	CV_104066	ULTRIUM V3
	CV_107424	ULTRIUM V3
	CV_107855	ULTRIUM V3
	CV_107856	ULTRIUM V3
	CV_107857	ULTRIUM V3
	CV_107858	ULTRIUM V3

The list of all the orphaned media appears in the right pane of Commcell Console.

The media icons give more information about status of any media. For more information about media icons, see Identifying Media Icons.

MOVE MEDIA TO LIBRARY

Use this option to move an orphaned media to a library. You can perform this operation for any orphaned media.

To move an orphaned media to a library:

1. From the right pane of the CommCell Console, right click the media that you want to move and click **Move to Library**.

   You can select multiple media simultaneously. Hold **Ctrl** key and select multiple media from the right pane of the CommCell Console. Then right click the selected media and click **Move to Library**.

2. From the **Move Media to Library** dialog box, select the library to which you want to move the media. This dialog box displays list of libraries which are compatible to the selected media.
3. Click **OK**. The media is moved to the selected library.

OTHER OPERATIONS

Depending upon the status of the media, some of the following operations are also available for each media:

- Export
- Recall Media
- View Contents
- Verify Media
- Move
- Delete
- Mark Media Good
- Prevent Export
- Update Barcode
- Properties
- Mark Media Reusable

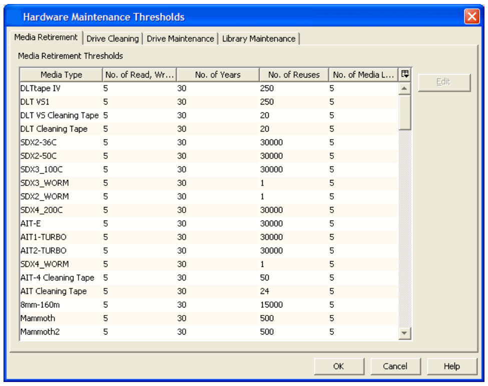
Back To Top

Hardware Maintenance

Topics | How To | Related Topics

MEDIA EXPIRATION THRESHOLD PARAMETERS

It is recommended to replace media before they begin to degrade. The Media Expiration Threshold Parameters helps you do this by keeping track of various types of media events (e.g., software error, reuses, etc.) for each media.



Media Retirement Thresholds

Media Type	No. of Read, Wr...	No. of Years	No. of Reuses	No. of Media L...
DLTtape IV	5	30	250	5
DLT VS1	5	30	250	5
DLT VS Cleaning Tape	5	30	20	5
DLT Cleaning Tape	5	30	20	5
SDX2-36C	5	30	30000	5
SDX2-50C	5	30	30000	5
SDX3_100C	5	30	30000	5
SDX3_WORM	5	30	1	5
SDX2_WORM	5	30	1	5
SDX4_200C	5	30	30000	5
AIT-E	5	30	30000	5
AIT1-TURBO	5	30	30000	5
AIT2-TURBO	5	30	30000	5
SDX4_WORM	5	30	1	5
AIT-4 Cleaning Tape	5	30	50	5
AIT Cleaning Tape	5	30	24	5
8mm-160m	5	30	15000	5
Mammoth	5	30	500	5
Mammoth2	5	30	500	5

Media Expiration Threshold Parameters can be viewed or modified from the **Media Retirement** tab of the **Hardware Maintenance Thresholds** dialog box. Use CommCell Console Control Panel to access the Hardware Maintenance Thresholds dialog box.

You can set event thresholds for each media type. (e.g., DLTtape IV.) In other words, you can decide how many events of each event type can occur before media from a particular media type exceeds its capacity for reliable operation.

> Refer to the manufacturer's documentation for the recommended maintenance criteria for each media type.

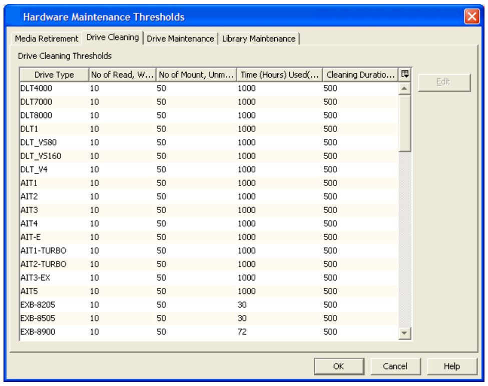
Whenever a media is obtained from the scratch pool, the system checks the threshold values, before attempting to write to the media. If the threshold values are exceeded, the media is marked as **Deprecated** and moved to the **Retired Media** pool. In addition, the system performs the following operations:

- Sends a message to the **Event Log**
- Generates the **Threshold Exceeded** alert, if configured

The above operations are also performed when the threshold parameters are exceeded in the course of usage, (i.e. when the media is in the **Assigned Media** pool). Note, however, the media will continue to remain in the **Assigned Media** pool, until the data in the media is pruned.

DRIVE CLEANING THRESHOLD PARAMETERS

To get optimal performance from your drives, you need to clean them periodically.



Drive Cleaning Thresholds

Drive Type	No of Read, W...	No of Mount, Unm...	Time (Hours) Used(...	Cleaning Duratio...
DLT4000	10	50	1000	500
DLT7000	10	50	1000	500
DLT8000	10	50	1000	500
DLT1	10	50	1000	500
DLT_VS80	10	50	1000	500
DLT_VS160	10	50	1000	500
DLT_V4	10	50	1000	500
AIT1	10	50	1000	500
AIT2	10	50	1000	500
AIT3	10	50	1000	500
AIT4	10	50	1000	500
AIT-E	10	50	1000	500
AIT1-TURBO	10	50	1000	500
AIT2-TURBO	10	50	1000	500
AIT3-EX	10	50	1000	500
AIT5	10	50	1000	500
EXB-8205	10	50	30	500
EXB-8505	10	50	30	500
EXB-8900	10	50	72	500

The Drive Cleaning Threshold Parameter helps you to keep track of various types of drive events that can occur before a drive is cleaned or fixed.

Drive Cleaning Threshold Parameters can be viewed and modified from the **Drive Cleaning** tab of the **Hardware Maintenance Thresholds** dialog box.

You can set event thresholds for each drive type. (e.g., DLT 7000.) In other words, you can decide how many events of each type can occur before a drive exceeds its capacity for reliable operation and must be cleaned or fixed. Such events include number of software and hardware errors and number of hours used.

When the number of events exceeds a preset threshold, the system performs the following operations:

- Sends a message to the **Event Log**
- Set the **Cleaning Required** option to **Yes** in the **Status** tab of **Drive Properties** dialog box, if the **Enable Auto-Cleaning** when threshold exceeds option is enabled in the **Drive** tab of the **Library Properties** dialog box. See Library Properties for more information on this option.
- Generates the **Threshold Exceeded** alert, if configured.
- Marks the drive **Offline** with the **Offline Reason** indicating that the drive cleaning threshold was exceeded and the drive **Broken** status is indicated as **Yes** in the **Drive Properties - Status** tab, if the **Mark Library/Drive Broken When Error Thresholds Exceeded** option is enabled in the **Library Properties** dialog box. See Library Properties for more information on this option.

> The system automatically cleans the drive when the drive cleaning threshold parameters are exceeded, if the **Enable Auto-Cleaning** option for the library is enabled. For information on the auto-cleaning option, see Enable Automatic Drive

Cleaning.

The actual usage values for the libraries and drives attached to a MediaAgent can be viewed by generating the **Library and Drive Report**.

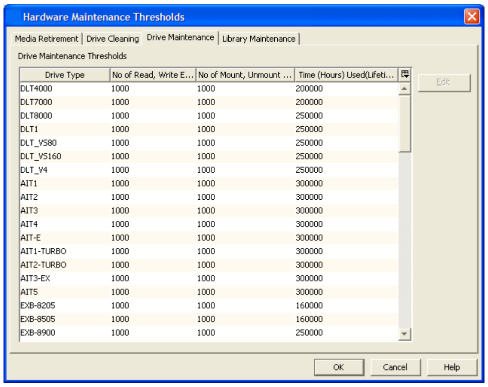
The threshold and usage information for each drive can be viewed in the **Odometer** tab of the **Drive Properties** dialog box.

Refer to the manufacturer's documentation for the recommended cleaning criteria for each drive type.

Drive Maintenance Threshold Parameters

To get optimal performance from your drives, you must replace them when necessary. Drive Maintenance Threshold Parameters helps you do this by keeping track of various types of drive events (e.g., software and hardware errors, read operations, etc.) for each drive.

Drive Maintenance Threshold Parameters can be viewed or modified from the **Drive Maintenance** tab of the **Hardware Maintenance Thresholds** dialog box.



Drive Type	No of Read, Write E...	No of Mount, Unmount ...	Time (Hours) Used(Lifeti...
DLT4000	1000	1000	200000
DLT7000	1000	1000	200000
DLT8000	1000	1000	250000
DLT1	1000	1000	250000
DLT_VS80	1000	1000	250000
DLT_VS160	1000	1000	250000
DLT_V4	1000	1000	250000
AIT1	1000	1000	300000
AIT2	1000	1000	300000
AIT3	1000	1000	300000
AIT4	1000	1000	300000
AIT-E	1000	1000	300000
AIT1-TURBO	1000	1000	300000
AIT2-TURBO	1000	1000	300000
AIT3-EX	1000	1000	300000
AIT5	1000	1000	300000
EXB-8205	1000	1000	160000
EXB-8505	1000	1000	160000
EXB-8900	1000	1000	250000

You can set event thresholds for each drive type. (e.g., DLT 7000.) In other words, you can decide how many events of each type can occur before a drive exceeds its capacity for reliable operation. When the number of events exceeds a preset threshold, the system performs the following operations:

- Sends a message to the **Event Log**
- Generates the **Threshold Exceeded** alert, if configured
- Marks the drive **Offline** with the **Offline Reason** indicating that a threshold was exceeded and the drive **Broken** status is indicated as **Yes** in the **Drive Properties - Status** tab, when the **Mark Library/Drive Broken When Error Thresholds Exceeded** option is enabled in the **Drive** tab of the **Library Properties** dialog box. See Library Properties for more information on this option.

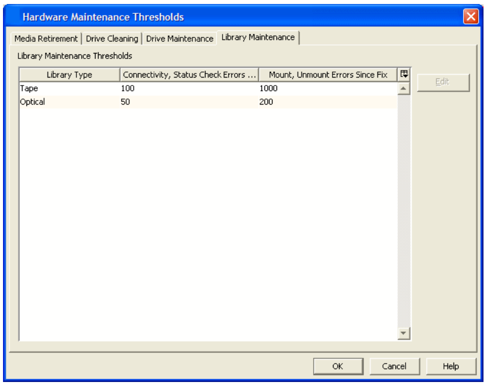
When you replace a drive, you must mark it as replaced. This will reset the appropriate event counters to zero.

Refer to the manufacturer's documentation for the recommended maintenance criteria for each drive type.

Library Maintenance Threshold Parameters

To get optimal performance from your libraries, you must replace them when necessary. Library maintenance threshold parameters helps you do this by keeping track of various types of library events (e.g., software and hardware errors) for each library.

Library Maintenance Threshold Parameters can be viewed or modified from the **Library Maintenance** tab of the **Hardware Maintenance Thresholds** dialog box.



Library Type	Connectivity, Status Check Errors ...	Mount, Unmount Errors Since Fix
Tape	100	1000
Optical	50	200

You can set event thresholds for each library type. (e.g., tape/optical.) In other words, you can decide how many events of each type can occur before a library exceeds its capacity for reliable operation. When the number of events exceeds a preset threshold, the system performs the following operations:

- Sends a message to the **Event Log**
- Generates the **Threshold Exceeded** alert, if configured
- .Marks the library **Offline** with the **Offline Reason** indicating that a threshold was exceeded in the **Library Properties - Status** tab, if the **Mark Library/ Drive Broken When Error Thresholds Exceeded** option is enabled in the **Library Properties** dialog box. See Library Properties for more information on this option.

When you fix/replace the library, you must mark the library as fixed. This will reset the appropriate event counters to zero. See Mark Library Fixed for more information.

Refer to the manufacturer's documentation for the recommended maintenance criteria for each library type.

Back to Top

Hardware Maintenance - How To

Topics | How To | Related Topics

Modify Media Expiration Threshold Parameters

MODIFY MEDIA EXPIRATION THRESHOLD PARAMETERS

Required Capability: See Capabilities and Permitted Actions

To modify media expiration threshold parameters:

1. From the **Tools** menu in the CommCell Console, click **Control Panel.**
2. Double-click **Hardware Maintenance**.
3. Click the Media Retirement tab.
4. Click the media type for which you wish to modify the thresholds, and then click **Edit**.
5. In the Media Expiration Threshold Parameters dialog box, modify the necessary threshold values, and then click **OK**.
6. Click **OK** in the **Hardware Maintenance Thresholds** dialog box to save the changes.

MODIFY DRIVE CLEANING THRESHOLD PARAMETERS

Required Capability: See Capabilities and Permitted Actions

To modify drive cleaning threshold parameters:

1. From the **Tools** menu in the CommCell Console, click **Control Panel.**
2. Double-click **Hardware Maintenance**.
3. Click the Drive Cleaning tab.
4. Click the drive type for which you wish to modify the thresholds, and then click **Edit**.
5. In the Drive Cleaning Threshold Parameters dialog box, modify the necessary threshold values, and then click **OK**.
6. Click **OK** in the **Hardware Maintenance Thresholds** dialog box to save the changes.

MODIFY DRIVE MAINTENANCE THRESHOLD PARAMETERS

Required Capability: See Capabilities and Permitted Actions

To modify drive maintenance threshold parameters:

1. From the **Tools** menu in the CommCell Console, click **Control Panel.**
2. Double-click **Hardware Maintenance**.
3. Click the Drive Maintenance tab.
4. Click the drive type for which you wish to modify the thresholds, and then click **Edit**.
5. In the Drive Maintenance Threshold Parameters dialog box, modify the necessary threshold values, and then click **OK**.
6. Click **OK** in the **Hardware Maintenance Thresholds** dialog box to save the changes.

MODIFY LIBRARY MAINTENANCE THRESHOLD PARAMETERS

Required Capability: See Capabilities and Permitted Actions

To modify library maintenance threshold parameters:

1. From the **Tools** menu in the CommCell Console, click **Control Panel.**
2. Double-click **Hardware Maintenance**.
3. Click the Library Maintenance tab.
4. Click the library type for which you wish to modify the thresholds, and then click **Edit**.

5. In the Library Maintenance Threshold Parameters dialog box, modify the necessary threshold values, and then click **OK**.
6. Click **OK** in the **Hardware Maintenance Thresholds** dialog box to save the changes.

MediaAgents

Topics | How To | Troubleshoot | Support | Related Topics

OVERVIEW

The MediaAgent manages the transmission of data between clients and backup media. There can be more than one MediaAgent within a CommCell.

The software supports MediaAgents on several Operating Systems, including support for MediaAgents in a clustered environment. (See System Requirements - MediaAgent for a list of supported MediaAgents and their requirements. See Support Information - Installation for information on cluster support for MediaAgents.)

See MediaAgent Deployment for information on installing the MediaAgent software.

Once installed, MediaAgents are displayed in the CommCell Browser as a sub-level under Storage Resources. You can perform several operations from the MediaAgent level and modify the properties associated with a MediaAgent. These are described in the following sections.

MEDIAAGENT OPERATIONS

LOG FILES

VIEW LOG

You can view the log files generated by a MediaAgent. The files that reside on a given computer may differ depending on the role of the computer in the CommCell (CommServe, MediaAgent, Client). A CommServe computer contains only the CommServe log files. A computer that is both a CommServe and a MediaAgent contains the log files of both entities. See Log Files for a detailed explanation of viewing log files.

SEND LOG

You can send the log files either from the CommCell Console, or from the Command line to email recipients as mails, or to a remote computer. You can also upload the log files to any existing FTP server. See Log Files for a detailed explanation of sending log files.

SCAN HARDWARE

You can scan the MediaAgent for any new hardware, and changes to existing hardware configurations, from the CommCell Console. This triggers a device detection at the operating system level for all corresponding CommCell computers, and reports the latest hardware configurations to the MediaAgent. See Scan a MediaAgent for Hardware Changes for step-by-step instructions.

INSTALL UPDATES

This option allows you to install updates from the CommServe Update Cache or a designated update cache on a remote client if multicache configuration is set up for use. See Install Updates to Specific Clients/MediaAgent for step-by-step instructions to install updates.

DE-CONFIGURE

To uninstall a MediaAgent from a CommServe, use the uninstall procedure as described in Uninstalling the MediaAgent.

If the uninstall fails to cleanup the MediaAgent information from the CommServe, use the **De-configure** option. Note that the De-configure option will not remove the files and registry entries associated with this MediaAgent.

The **De-configure** option performs the following tasks:

- Cleans up all the information about the MediaAgent in the CommServe database
- Releases the license associated with the MediaAgent
- Releases the licenses associated with the libraries or stand-alone drives attached to the MediaAgent. However, licenses associated with a library whose media changer is not controlled by this MediaAgent (e.g. SAN devices, shared libraries) will not be released.

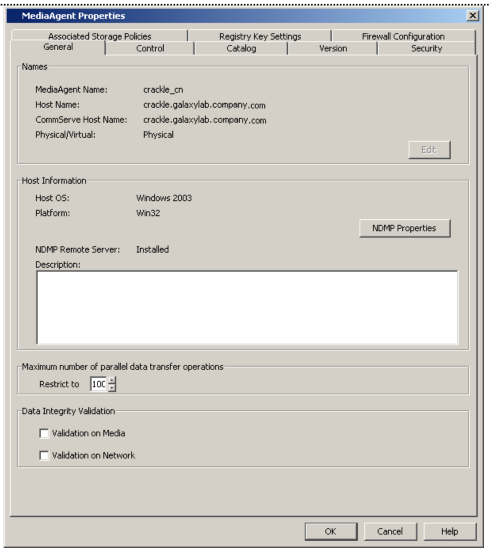
For a detailed explanation on de-configuring MediaAgents, see Deconfiguring Agents.

USER ALERTS

Alerts allow you to set e-mail notifications to MediaAgent related events. For a detailed explanation of Alerts, see Alerts and Monitoring.

MEDIAAGENT PROPERTIES

GENERAL



Names

MediaAgent Name: crackle_cn
Host Name: crackle.galaxylab.company.com
CommServe Host Name: crackle.galaxylab.company.com
Physical/Virtual: Physical

Host Information

Host OS: Windows 2003
Platform: Win32
NDMP Remote Server: Installed
Description:

Maximum number of parallel data transfer operations

Restrict to 100

Data Integrity Validation

□ Validation on Media
□ Validation on Network

The MediaAgent properties can be viewed from the **General** tab of the **MediaAgent Properties** dialog box.

NAMES

General information includes the MediaAgent name, host name, the name of the CommServe to which the MediaAgent is attached, and whether the MediaAgent is installed in the Physical or in the Virtual machine in a clustered environment.

You can change the name of the Client/MediaAgent computer if the Host name is changed. See Name Management for more information.

Do not use spaces when specifying a new name for the Client.

HOST INFORMATION

Information includes the MediaAgent's operating system and platform. If necessary you can use the description field to record additional information about the MediaAgent. Click on **NDMP Properties** to edit the details of the NDMP Server host filer.

MAXIMUM NUMBER OF PARALLEL DATA TRANSFER OPERATIONS

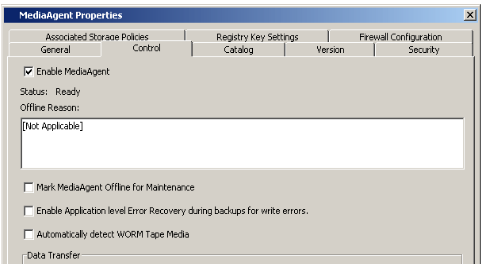
This feature allows you to set the maximum number of concurrent read/write operations to the MediaAgent. This value controls the maximum number of data streams that can be managed by the MediaAgent. See Set the Maximum Number of Parallel Data Transfer Operations for a MediaAgent for step-by-step instructions.

The default number of concurrent read/write operations to a MediaAgent is 25. This value can be set between 1 and 75. If Optimize for Concurrent LAN Backup option is enabled from the Control tab, then the default is set to 100 and this value can be set to a maximum of 200 (only on Windows and Unix).

DATA INTEGRITY VALIDATION

The integrity of data protection operations can be ensured by enabling Data Integrity Validation at the MediaAgent. Data Integrity Validation can be used to verify the data stored in the media as well as the data transferred over network. See Data Integrity Validation for more information.

CONTROL



☑ Enable MediaAgent

Status: Ready

Offline Reason:

[Not Applicable]

□ Mark MediaAgent Offline for Maintenance

□ Enable Application level Error Recovery during backups for write errors.

□ Automatically detect WORM Tape Media

Data Transfer

MEDIAAGENT CONTROL

The following options for controlling the MediaAgent is provided:

- **Enable or disable the MediaAgent**

  You can enable or disable a MediaAgent. When a MediaAgent is disabled, it is not used, even if it is physically available. (See Enable (or Disable) a MediaAgent for step-by-step instructions.)

  MediaAgents and data protection and recovery operations for clients can be enabled or disabled in bulk with the EnableDisableComputers command line utility in the Resource Pack. The tool can be applied to all MediaAgents and clients, or for a select targeted group.

- **Status of the MediaAgent**

  The status of the MediaAgent is displayed to indicate whether the MediaAgent software is online or offline, and if offline, the reason for the offline status is also displayed.

  The system checks for the status of the MediaAgent and updates the information based on the values established in the **LAN-Free MediaAgent liveliness check interval in Minutes** and **LAN MediaAgent liveliness check interval in Minutes** options from the Media Management Configuration (Service Configuration) dialog box available in the **Control Panel**.

- **Mark MediaAgent Offline for Maintenance**

  You can enable this option when you wish to perform routine or other maintenance tasks on devices. This option is available in the MediaAgent, Library and Drive levels and you can appropriately enable them where needed.

  Data protection, data recovery and auxiliary copy operations will not use the associated MediaAgent/Library/Drive, depending on where the option is enabled. However, other administrative tasks on the devices such as Full Scan, Drive Cleaning, Verify Media etc. can be performed, if required.

  When this option is enabled, the system will automatically select an alternate resource (MediaAgent/Library/Drive) if Alternate Data Paths (GridStor) is enabled. If alternate resources are not available, data protection, data recovery and auxiliary copy will remain in the `Waiting` state in the **Job Controller** and will automatically resume when you re-enable the appropriate MediaAgent/Library/Drive.

  See Mark MediaAgent/Library/Drive Offline for Maintenance for step-by-step instructions.

- **Enable Application level Error Recovery during backups for write errors**

  You can enable this option to indicate that the MediaAgent should perform error recovery by readjusting the tape position and re-write the last block when IO error occurs. This option maybe enabled when data protection jobs fail due to SCSI related write errors in the library.

  However, note that extreme caution must be exercised while selecting this option as it severely impacts the performance of the MediaAgent.

  As most write errors are due to hardware failures, steps must be taken to fix the hardware instead of enabling this option. This option may be temporarily enabled to ensure that the current data protection jobs are successful until the hardware is fixed.

  Note that the error recovery attempts may not be successful if the hardware errors persists.

- **Data Transfer**

  Optimize for Concurrent LAN Backups

  This option can be enabled when the MediaAgent is used for concurrent data protection operations from a large number of clients. For example, if you have 25 clients concurrently using the MediaAgent for 50 or more data transfer streams in a specific operation window, it is recommended that you enable this option Enabling this option will help to optimize the Operating System resources on the MediaAgent.

  See Maximum number of parallel data transfer operations for the maximum number of parallel read/write operations with the Optimize for Concurrent LAN Backups option enabled.

  See MediaAgents - Supported Features, Agents and Devices for information on the MediaAgents that support this option.

  See Optimize the MediaAgent for Concurrent LAN Backups for step-by-step instructions.

- **Device Detection**

  Automatic Update of SCSI ID during live operation

  In the SAN environment, the SCSI ID of a device may get changed due to a HBA failover or if the a hardware component in the SAN is reset. In such a situation, read/write requests to the media in the device may fail, resulting in job failures. However, if this option is enabled, the system will automatically scan the device and update the SCSI ID and the job will be re-tried in the established retry interval.

  This option also includes the following sub-options:

  - **SCSI/SAN device scan interval n hour(s)**

    This option specifies the time interval that must be used for successive retry operations for SCSI ID updates. For example, if a SCSI ID update is performed after a read/write failure and a second read/write failure occurs almost immediately or within the specified time interval, the system will not perform the SCSI ID update. The system will scan for SCSI ID updates only when a error occurs after the specified time interval. It is recommended that the time interval be set to 30 minutes or more, as running jobs could go into pending, when the SCSI ID is updated.

  - **Mark drive inaccessible on error and perform status check according to device scan interval**

    When enabled, this option marks the drive controller offline when the SCSI ID for a device is changed. (This can be viewed from the **Drive Properties - Drive Controller** tab, where the **Drive Accessible** will be displayed as No.)

    The device detection will be performed once every 24 hours. This property can be modified using the **SCSI/SAN device scan interval n hours(s)** option in the MediaAgent Properties. Note that if the value established in **MediaAgent Properties** is less than 24 hours, the system automatically defaults to 24 hours.

    If you want to perform this operation more frequently create the nDisabledDriveDetectIntervalMin registry key. Once created, this registry key will override the setting established in the **MediaAgent Properties**.

    The device detection will be repeated for 7 days. If these drives are not accessible even after 7 days, the drives will be marked as accessible. (If the drive continues to have a problem, the subsequent job accessing the drive will once again cause it to be marked as inaccessible.) If necessary the nDisabledDriveMaxDetectionRetryHours registry keys can be created to change the number of days the device detection will be repeated.

    > On NetWare MediaAgents both these keys must be manually created with a value greater than 0 to enable this feature.

- **Native Driver Support**

  To communicate with the tape devices, you can use the pass-through driver provided by the MediaAgent, or the native drivers provided by the operating system. When this option is selected the native driver is used. This option is supported by all UNIX MediaAgents. By default, this option is enabled on all

Unix MediaAgents. Disable this option, if you do not want to use the native drivers.

See Also:

- Tape Spanning failure on AIX MediaAgents with Native Drivers
- Job Failures in Solaris MediaAgents using Native Drivers

Send pass-thru commands to Atape

When using native driver support, use this option to enable MediaAgent to send pass-through commands to Atape device drivers.

- **Automatically detect WORM Tape Media**

  When enabled, this option automatically detects WORM media when it is used in a drive. This option must be enabled if you plan to use WORM media in the libraries attached to the MediaAgent. (Check the drive manufacturer's documentation to ensure that both the drive model and firmware must support the usage of WORM media.)

- **Enable retry on network errors**

  When enabled, this option allows you to set the retry options in case of network errors.

  - **Retry Frequency (seconds)**

    The interval (in seconds) at which the Job Manager will continuously check for network connectivity.

  - **Retry Count**

    The number of times the Job Manager will check for network connectivity.

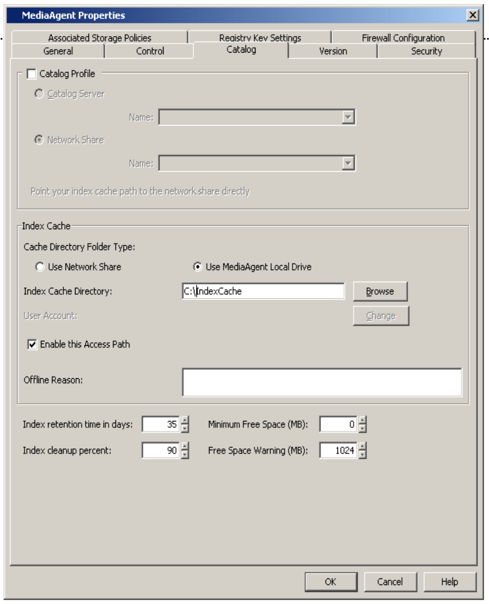
  See Enable/Disable Robust Network Layer for step-by-step instructions. See Robust Network Layer for more details.

CATALOG

A MediaAgent’s Index cache information be viewed from the **Catalog** tab of the **MediaAgent Properties** dialog box. You can view or modify the following information associated with the MediaAgent’s index cache configuration:

- Catalog Profile
- Index Cache Directory
- Index Retention Criteria

For a detailed explanation of a MediaAgent's Index Cache, see Index Cache.



☐ Catalog Profile

○ Catalog Server

Name:

● Network Share

Name:

Point your index cache path to the network share directly

Index Cache

Cache Directory Folder Type:

○ Use Network Share ● Use MediaAgent Local Drive

Index Cache Directory: C:\IndexCache

User Account:

☑ Enable this Access Path

Offline Reason:

Index retention time in days: 35 Minimum Free Space (MB): 0

Index cleanup percent: 90 Free Space Warning (MB): 1024

VERSION

The **Version** tab of the **MediaAgent Properties** dialog box displays the version number of the MediaAgent software that is installed on the MediaAgent computer. It also displays all post-release Service Packs and Automatic Updates that may have been installed on the MediaAgent. It also displays the location of the update information.

For a detailed explanation of the version information, see Version.

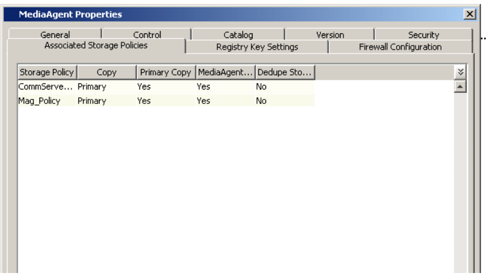
SECURITY

Security allows you to associate the MediaAgent with one or more CommCell user groups.

For a detailed explanation of security, see User Administration and Security.

ASSOCIATED STORAGE POLICIES

The **Associated Storage Policies** tab provides information about all the storage policy and their copies associated with a MediaAgent. This information is useful when you deconfigure a MediaAgent, as all the storage policy copies associated with the MediaAgent can be re-pointed or deleted prior to deconfiguring the MediaAgent.



Storage Policy	Copy	Primary Copy	MediaAgent...	Dedupe Sto...
CommServe...	Primary	Yes	Yes	No
Mag_Policy	Primary	Yes	Yes	No

REGISTRY KEY SETTINGS

The **Registry Key Settings** tab enables you to add, edit, or delete registry keys for Windows and unix MediaAgents. For Netware, you must use the manual process. See Managing Registry Keys From the CommCell Console for more information.

FIREWALL CONFIGURATION

If a firewall separates MediaAgent and other CommCell components it communicates, then you can specify the incoming and outgoing connectivity details between MediaAgent and the components in the **Firewall Configuration** tab. See Firewalls for more information on supported firewall various firewall scenarios and their configuration.

IMPORTANT CONSIDERATIONS

AUDIT TRAIL

Operations performed with this feature are recorded in the Audit Trail. See Audit Trail for more information.

Back To Top

MediaAgents - How To

Topics | How To | Troubleshoot | Support | Related Topics

SET THE MAXIMUM NUMBER OF PARALLEL DATA TRANSFER OPERATIONS FOR A MEDIAAGENT

Required Capability: Capabilities and Permitted Actions

To set the maximum number of parallel data transfer operations for a MediaAgent:

1. From the CommCell Browser, right-click the MediaAgent for which you wish to set the number of parallel data transfer operations, and then click **Properties**.

2. Click the General tab.
3. In the **Maximum number of parallel data transfer operations** area, set the number of streams in the **Restrict To** box.
4. Click **OK** to save the configuration.

CONFIGURE NDMP PROPERTIES

Required Capability: Capabilities and Permitted Actions

▶ To configure the NDMP Remote Server properties:

1. In the CommCell Browser, expand the **MediaAgents** icon, right-click a MediaAgent and select **Properties**.
2. Click the **NDMP Properties** button from the General tab.
3. In the **NDMP Server Hostname** field, enter the Hostname of the MediaAgent (this should already be populated by default.)
4. Check **Change Password**, and in the **NDMP Login** and **NDMP Password** fields, enter the Administrator Account Name and Password for the MediaAgent computer.
5. In the **Listen Port** field, enter the Port number specified during the install of the EMC CBRM software (we suggest 10002).
6. Click the **Detect** button. A successful detection will populate the **Vendor** and **Firmware Revision** fields.
7. Click **OK** to save the configuration.

ENABLE (OR DISABLE) A MEDIAAGENT

Required Capability: Capabilities and Permitted Actions

▶ To enable or disable a MediaAgent:

1. From the CommCell Browser, click the **MediaAgents** icon. All the MediaAgents available in the CommCell are displayed on the right-pane of the CommCell Browser.
2. Right-click the MediaAgent that you wish to enable or disable, and then click **Properties**.
3. From the Control tab of MediaAgent Properties, select the **Enable MediaAgent** option to bring the MediaAgent online. Clear this option to take the MediaAgent offline.
4. Click **OK** to save the configuration.

VIEW THE MEDIAAGENT OFFLINE REASON

Required Capability: Capabilities and Permitted Actions

▶ To view the status of a MediaAgent:

1. From the CommCell Browser, click the **MediaAgents** icon. All the MediaAgents available in the CommCell are displayed on the right-pane of the CommCell Browser.
2. Right-click the MediaAgent for which you wish to view the status, and then click **Properties**.
3. The MediaAgent's online or offline status can be viewed from the In the Control tab of MediaAgent Properties dialog box.
4. Note that if the Media is *Offline* the offline reason is also displayed.

OPTIMIZE THE MEDIAAGENT FOR CONCURRENT LAN BACKUPS

Required Capability: Capabilities and Permitted Actions

▶ To optimize a MediaAgent for concurrent LAN backups:

1. From the CommCell Browser, click the **MediaAgents** icon. All the MediaAgents available in the CommCell are displayed on the right-pane of the CommCell Browser.
2. Right-click the MediaAgent that you wish to optimize for concurrent LAN backups and then click **Properties**.
3. Click the Control tab.
4. Click and choose the **Optimize for concurrent LAN backups** to enable the option. (Clear this option to disable.)

5. Click **OK** to save the configuration.

   Subsequent data protection operations using the MediaAgent use the selected mechanism.

ENABLE (OR DISABLE) AUTOMATIC DETECTION OF WORM MEDIA

Required Capability: Capabilities and Permitted Actions

➤ To enable or disable automatic detection of WORM media:

1. From the CommCell Browser, click the **MediaAgents** icon. All the MediaAgents available in the CommCell are displayed on the right-pane of the CommCell Browser.
2. Right-click the MediaAgent that you wish to enable (or disable) automatic detection of WORM media and then click **Properties**.
3. Click the Control tab.
4. Click and choose the **Automatically detect WORM Tape Media** option to enable automatic detection. (Clear the option to disable it.)
5. Click **OK** to save the configuration.

MARK MEDIAAGENT/LIBRARY/DRIVE OFFLINE FOR MAINTENANCE

Required Capability: Capabilities and Permitted Actions

➤ To mark MediaAgent/Library/Drive Offline for Maintenance:

1. From the CommCell Browser, right-click the MediaAgent/Library/ Drive that you wish to mark offline for maintenance, and then click **Properties**.
2. Select one or more of the following options as appropriate:
   - To mark a MediaAgent offline for maintenance: Click the Control tab and then click and enable the **Mark MediaAgent Offline for Maintenance** option.
   - To mark a library offline for maintenance: Click the Status tab and then click and enable the **Mark Library Offline for Maintenance** option.
   - To mark a drive offline for maintenance: Click the Status tab and then click and enable the **Mark Drive Offline for Maintenance** option.
3. Click **OK** to save the configuration.

   Subsequent data protection, data recovery and auxiliary copy operations will not use the associated MediaAgent/Library/Drive.

CREATE A NETWORK SHARE PROFILE

Required Capability: Capabilities and Permitted Actions

➤ To create a network share profile for index cache sharing:

1. From the CommCell Browser, right-click the CommServe, click **Control Panel,** and select **Shared Catalog Configuration**.

   Alternatively, from the CommCell Browser, right-click the MediaAgent, and click **Configure.**
2. From the Shared catalog Configuration dialog box, click **Add** to create a Network Share Profile.
3. Enter the name of the Profile to be created in **Profile Name** box.
4. Select the type of index share:
   - **Network Share** - Network share directs the index cache to a common network location.
5. In the **Profile Properties** area, specify the following retention criteria for the shared index cache.
   - **Index Retention Time in days** - Select the number of days after which an index cache can be removed. This criteria is used for the purpose of removing index cache.
   - **Index Cleanup Percent** - Select the disk percentage used to remove the index cache.
   - **Minimum Free Space (MB)** – Select the total amount of free space that must be available at all times in the index cache.
   - **Free Space Warning (MB)** – Select the amount of free space in the index cache. If the amount of free space falls below the specified amount, the MediaAgent generates an event message and generates the MediaAgents (Disk Space Low) alert, if configured.
6. Click **OK** to create the profile. You can use this profile on a MediaAgent to share the index cache.

CONFIGURE A MEDIAAGENT FOR INDEX CACHE SHARING

Required Capability: Capabilities and Permitted Actions

To configure a MediaAgent for index cache sharing:

1. From the CommCell Browser, right-click the MediaAgent you wish to share the index cache and click **Properties**.
2. From the **MediaAgent Properties** window click the Catalog tab.
3. Select **Catalog Profile** option to enable index cache sharing.
4. To use a Network Share, click **Network Share** and select a Network Share profile from the list. All **Network Share** profiles created from the **Shared Catalog Configuration** window will be available for selection.

   Point your index cache to the network share location.

   For Windows MediaAgents:

   - Select **Use Network Share** - if the index cache will reside on a network share.
   - In the **Index Cache Directory** box, type the path to the index cache directory or use the **Browse** button to select the path.
   - Click the **Change** button. In the Change User Account dialog box, type the user account and password that must be used to access the Index Cache and then click **OK**.
   - It is highly recommended that the option **Enable Intermediate Index Cache Directory** be used when configuring Index Cache on a network share. With this option turned on the index is written to the local disk first and at commit points uploaded to the Network share. This will avoid failures due to network disruptions/failures writing to the index on the network share.
   - Click **OK** to save the configuration.

   For Unix MediaAgents:

   - In the **Index Cache Directory** box, type the path to the index cache directory or use the **Browse** button to select the path. If the index cache resides on a network share, then this will be the path to network index cache mounted locally.
   - It is highly recommended that the option **Enable Intermediate Index Cache Directory** be used when configuring Index Cache on a network share. With this option turned on the index is written to the local disk first and at commit points uploaded to the Network share. This will avoid failures due to network disruptions/failures writing to the index on the network share.
   - Click **OK** to save the configuration.
5. The index cache is shared.
6. Now this index is available to be shared from other MediaAgents.
7. Right-click *another MediaAgent* that will share the index and then click **Properties**.
8. Click the the Catalog tab.
9. Select **Catalog Profile** option to enable index cache sharing.
10. To use a Network Share, click **Network Share** and select a Network Share profile from the list. All **Network Share** profiles created from the **Shared Catalog Configuration** window will be available for selection.

    Point your index cache to the network share location.

    For Windows MediaAgents:

    - Select **Use Network Share** - if the index cache will reside on a network share.
    - **Use MediaAgent Local Drive** - if the index cache will reside on a local drive.
    - In the **Index Cache Directory** box, type the path to the index cache directory or use the **Browse** button to select the path.
    - Click the **Change** button. In the Change User Account dialog box, type the user account and password that must be used to access the Index Cache and then click **OK**.
    - It is highly recommended that the option **Enable Intermediate Index Cache Directory** be used when configuring Index Cache on a network share. With this option turned on the index is written to the local disk first and at commit points uploaded to the Network share. This will avoid failures due to network disruptions/failures writing to the index on the network share.
    - Click **OK** to save the configuration.

    For Unix MediaAgents:

    - In the **Index Cache Directory** box, type the path to the index cache directory or use the **Browse** button to select the path. If the index cache resides on a network share, then this will be the path to network index cache mounted locally.
    - Click **OK** to save the configuration.
11. Repeat steps 8 -10 on all the MediaAgents that share the index cache.

Unshare a Shared Index Cache

Before You Begin

- Ensure that the MediaAgent is not defined as an alternate data path candidate in any of the storage policy copies. If the MediaAgent is used as candidate, the system will automatically prevent you from unsharing the index cache.
- For Unix MediaAgents, if the index cache resides on a network share, you have to manually mount the drive containing the index cache to the local machine to be able to create a shared index cache. Also note down the local mount path.

Required Capability: Capabilities and Permitted Actions

To unshared a shared index cache:

1. From the CommCell Browser, right-click the MediaAgent for which you wish to unshare the shared index cache and then click **Properties**.
2. From the Catalog tab, uncheck the **Catalog Profile** option. The index cache is no longer shared.
3. If you were using a Network Share, then you will have to provide a local path for the index cache. Perform one of the following:

   For Windows MediaAgents:

   - Select **Use Network Share** if the index cache will reside on a network share, or select **Use MediaAgent Local Drive** if the index cache will reside on a local drive.
   - In the **Index Cache Directory** box, type the path to the index cache directory or use the **Browse** button to select the path.
   - If the MediaAgent resides on a Network Share, click the **Change** button. In the Change User Account dialog box, type the user account and password that must be used to access the Index Cache and then click **OK**.

   For Unix MediaAgents:

   - In the **Index Cache Directory** box, type the path to the index cache directory or use the **Browse** button to select the path. If the index cache resides on a network share, then this will be the path to network index cache mounted locally.
4. Click **OK** to save the configuration.

Move an Index Cache

Before You Begin

- For Unix MediaAgents, if the index cache resides on a network share, you have to manually mount the drive containing the index cache to the local machine to be able to create a shared index cache. Also note down the local mount path.

Required Capability: Capabilities and Permitted Actions

To move an index cache:

1. From the CommCell Browser, right-click the MediaAgent for which you wish to move the index cache and then click **Properties**.
2. Click the Catalog tab.
3. Provide details in the **Index Cache** area.

   For Windows MediaAgents:

   - Select **Use Network Share** if the index cache will reside on a network share, and select **Use MediaAgent Local Drive** if the index cache will reside on a local drive.
   - In the **Index Cache Directory** box, type the path to the index cache directory or use the **Browse** button to select the path.
   - If the MediaAgent resides on a Network Share, click the **Change** button. In the Change User Account dialog box, type the user account and password that must be used to access the index cache and then click **OK**.

   For Unix MediaAgents:

   - In the **Index Cache Directory** box, type the path to the index cache directory or use the **Browse** button to select the path. If the index cache resides on a network share, then this will be the path to network index cache mounted locally.
4. Click **OK** to save the configuration.
5. If the index is moved from a local drive to a network share, a **Confirm** prompt is displayed, asking you whether you wish to copy the index cache. Click one of the following:
   - **Yes** to copy the index cache to the new index cache folder.
   - **No** to move the index cache without copying the index cache folder. In this case subsequent jobs may result in index restore operation from the media.
6. The index cache is moved to the new folder.

NOTES

- It is important that you do not change the Name of the Profile when moving a shared index cache.
- On Windows MediaAgents, the original directory may have to be manually deleted to free the disk space.
- Index Cache can only be moved when no index jobs like Auxiliary Copy, Disaster Recovery Backups, Deduplication Backups, etc. are running.
- If you wish to manually move the index cache, see Manually Relocate the Index Cache.
- If the index cache contains SnapProtect backup data, you will have to Manually Relocate the Index Cache.

MOVE A SHARED INDEX CACHE

Before You Begin

- For unix MediaAgents, if the index cache resides on a network share, you have to manually mount the drive containing the index cache to the local machine to be able to create a shared index cache. Also note down the local mount path.

Required Capability: Capabilities and Permitted Actions

To move a shared index cache:

1. From the CommCell Browser, right-click *any one* of the MediaAgents that share the shared index cache and then click **Properties**.
2. Click the Catalog tab.

   For Windows MediaAgents:

   - Select **Use Network Share** if the index cache will reside on a network share, and select **Use MediaAgent Local Drive** if the index cache will reside on a local drive.
   - In the **Index Cache Directory** box, type the path to the index cache directory or use the **Browse** button to select the path.
   - If the MediaAgent resides on a Network Share, click the **Change** button. In the Change User Account dialog box, type the user account and password that must be used to access the Index Cache and then click **OK**.

   For Unix MediaAgents:

   - In the **Index Cache Directory** box, type the path to the index cache directory or use the **Browse** button to select the path. If the index cache resides on a network share, then this will be the path to network index cache mounted locally.
3. Click **OK** to save the configuration.
4. Repeat the above steps *on all* the MediaAgents that share the index cache. If this is not done, the index cache will be turned offline after 30 minutes, and all the jobs accessing the MediaAgents that share this index cache may fail as a result.

NOTES

- It is important that you do NOT change the **Name** of the Network Profile when moving a shared index cache.
- On Windows MediaAgents, the original directory may have to be manually deleted to free the disk space.
- Index Cache can only be moved when no index jobs like Auxiliary Copy, Disaster Recovery Backups, Deduplication Backups, etc. are running.

SET THE INDEX RETENTION CRITERIA FOR NETWORK SHARE PROFILES

Required Capability: Capabilities and Permitted Actions

To establish the index retention criteria for network share profiles:

1. From the CommCell Browser, click the **MediaAgents** icon. All the MediaAgents available in the CommCell are displayed on the right-pane of the CommCell Browser.
2. Right-click the MediaAgent whose index cache parameters you wish to modify, and then click **Properties**.
3. Click the Catalog tab of **MediaAgent Properties** dialog box.
4. You can change the following retention parameters:
   - Index retention time in days
   - Index cleanup percent
   - Minimum Free Space in MB
   - Free Space Warning in MB
5. Click **OK** to save the configuration.

VIEW THE SOFTWARE VERSION

To view the Software Version:

1. From the CommCell Browser, click the **CommServe**, **Client**, **Agent**, **MediaAgent**, or **Enabler** for which you wish to view the version, and then click **Properties**.
2. Click the Version tab.

   The component version and post release service pack, additional updates and missing updates are displayed.

RELEASE LICENSE FOR MEDIAAGENT

Required Capabilities: Capabilities and Permitted Actions

Administrative Management capability cannot be used to release the license from the MediaAgent level.

Before you Begin:

- To release license for MediaAgent, ensure that all the storage policies or copies associated with the configured libraries (or drive pools) in the MediaAgent are deleted or re-associated to another MediaAgent.

To release license for client, MediaAgent, agent, or enabler:

1. In the CommCell Browser, right-click the name of the MediaAgent you want to release license, and select **Release license for Media Agent**.
2. A popup warning message appears.

   Click **OK** to continue.
3. Another popup message then appears.

   Click **Yes** to continue with the deconfiguration or **No** to abort.
4. If releasing a license is unsuccessful, a number of popup messages appears. In some cases, the message requests that you take some corrective action.

   For example, the message might advise you to ensure that there are no jobs running on the agent.

   In such case, click **OK** and take the appropriate action. Then repeat the process.

If releasing a license is successful, the tree element is dimmed and available for deletion.

MOVE A LIBRARY TO ANOTHER MEDIAAGENT WITHOUT DATA LOSS

In some situations you may have the need to move a library from one MediaAgent to another due to re-configuration or other requirements.

The following procedure provides step-by-step instructions on how to perform this operation.

1. Detach the library and attach it to the new MediaAgent and make sure that the hardware is visible to the operating system. See Driver Configurations for more information.
2. Open the CommCell Console and change the name of the MediaAgent associated with the library. See Change the MediaAgent (Host) Associated with a Library for more information.
3. If necessary run a quick backup to verify that the devices are functioning correctly.

MOVE A MEDIAAGENT WITHOUT DATA LOSS

In some situations you may have the need to move a MediaAgent from one computer to another. For example:

- You may want to move the MediaAgent to another computer when you move the pilot version of the software to the production environment.
- You may want to separate the MediaAgent from a CommServe, if they were installed together.
- You may want to move a MediaAgent to a more powerful computer or such similar re-configuration needs.

You will require an additional MediaAgent license to perform this operation.

The following procedure provides step-by-step instructions on how to perform this operation.

1. Detach the library and attach it to the new computer and make sure that the hardware is visible to the operating system. See Driver Configurations for more information.

2. Install the MediaAgent software in the new computer. See MediaAgent Deployment for more information.
3. Open the CommCell Console and change the name of the MediaAgent associated with the library that was configured in the old MediaAgent. See Changing the MediaAgent (Host) Associated with a Library for more information.
4. If the index cache is configured in the old MediaAgent, move the index cache to the new MediaAgent. (See Move an Index Cache for step-by-step instructions.)
5. If necessary run a quick backup to verify that the devices are functioning correctly.
6. Uninstall the MediaAgent software from the original computer. See Uninstall Components for more information.

    WARNING

    Do not deconfigure the library at any point.

    Also do not uninstall the old MediaAgent until the devices start functioning in the new MediaAgent.

SEPARATE THE COMMSERVE FROM A COMMSERVE-MEDIAAGENT COMPUTER

In some situations you may want to separate the CommServe from a MediaAgent computer, (with or without a File system *i*DataAgent) if they were installed together. For example, you may want to move the CommServe to a more powerful computer or such similar re-configuration needs.

The following procedure provides step-by-step instructions on how to perform this operation.

You can also use this procedure to relocate a CommServe and MediaAgent which are installed together, to two separate computers.

You will require an additional MediaAgent license to perform this operation.

SOURCE COMPUTER

1.	Copy the index cache folder (and the job results folder if the (File system *i*DataAgent is installed) to another location.	
2.	Perform a Disaster Recover Backup. Verify and ensure that the Disaster Recovery Backup completes successfully. Also note down the location of the disaster recovery backup file. (For a more detailed discussion, see Phases of Disaster Recovery Backups.)	See Starting a Disaster Recovery Backup for step-by-step instructions.
3.	Uninstall the software from the original computer.	See Uninstalling Components for more information.
	WARNING Do not deconfigure the libraries (tape/optical/disk libraries, etc.) when you uninstall the MediaAgent software.	

ESTABLISHING THE NEW COMMSERVE COMPUTER

4.	Install only the CommServe software in the new computer.	See CommServe Deployment for information on installing the CommServe software.
5.	Restore the CommServe database using the CommServe Disaster Recovery Tool.	See Restore a Disaster Recovery Backup for step-by-step instructions.
6.	Change the name of the CommServe computer using the CommServe Disaster Recovery Tool.	See Change the Name of the CommServe Computer for step-by-step instructions.
7.	Inform the Client and MediaAgent computers of the new CommServe name. This can be done from the `CommCell Console`.	See Informing Clients of CommServe Name Change for step-by-step instructions.

ESTABLISHING THE NEW MEDIAAGENT COMPUTER

8.	Install only the MediaAgent software in the old computer. (You can also relocate the MediaAgent to another computer, if necessary.)	See MediaAgent Deployment for more information.
9.	During MediaAgent installation make sure to specify the index cache to the location in which it was copied in step 1. If you are unable to do so, perform the steps described in Manually Relocate the Index Cache.	
10.	Open the CommCell Console and change the MediaAgent name associated with the library.	See Changing the MediaAgent (Host) Associated with a Library for step-by-step instructions.
	If you have a disk library, make sure that the mount path is pointing to the appropriate location. If necessary move the mount path to the appropriate location and then change the location of the mount path.	See Move a Mount Path for step-by-step instructions.

11.	Deconfigure the original MediaAgent from the CommCell Console.	See Deconfigure a Client, MediaAgent, Agent, or Enabler for step-by-step instructions.

ESTABLISHING THE FILE SYSTEM *i*DATAAGENT IN THE MEDIAAGENT COMPUTER (IF IT WAS ORIGINALLY INSTALLED)

12.	Export the metadata records associated only with this client on the CommServe.	See Export Data from the Source CommCell for step-by-step instructions.
13.	Deconfigure the Client from the CommCell Console.	See Deconfigure a Client, MediaAgent, Agent, or Enabler for step-by-step instructions.
14.	Delete the Client in the CommCell Console.	See Delete a Client Computer for step-by-step instructions.
15.	Import the metadata records (that was exported in step 12) associated with the client computer in the CommServe.	See Import Data on the Destination CommCell for step-by-step instructions.
16.	Reinstall the file system *i*DataAgent on the computer.	See Deployment - Windows File System iDataAgent for more information.

ENABLE/DISABLE ROBUST NETWORK LAYER

Required Capability: Capabilities and Permitted Actions

To enable or disable the Robust Network Layer feature:

1. From the CommCell Console, right click on a client, and select **Properties** from the pop-up menu. Select the Client Computer Properties (Advanced) tab.

   Alternatively, right click on a MediaAgent and select **Properties** from the pop-up menu. Select the MediaAgent Properties (Control) tab.
2. Select the **Enable retry on network errors** option to enable the feature. Deselect it to disable the feature.
3. Click **OK**.

CHANGE ROBUST NETWORK LAYER CONFIGURATION

Required Capability: Capabilities and Permitted Actions

To change the Robust Network Layer configuration:

1. From the CommCell Console, right click on a client, and select **Properties** from the pop-up menu. Select the Client Computer Properties (Advanced) tab.

   Alternatively, right click on a MediaAgent and select **Properties** from the pop-up menu. Select the MediaAgent Properties (Control) tab.
2. Select the **Enable retry on network errors** option to enable the feature. Deselect it to disable the feature. If enabled, you may configure the following:
   - **Retry Frequency (seconds)**: The interval (in seconds) at which the Job Manager will continuously check for network connectivity. Default is set at 30 seconds.
   - **Retry Count**: The number of times the Job Manager will check for network connectivity. Default is set at 40.
3. Click **OK**.

SCAN A MEDIAAGENT FOR HARDWARE CHANGES

Required Capability: Capabilities and Permitted Actions

To scan the MediaAgent for hardware changes:

1. From the CommCell Console, right click on a MediaAgent and select the **Scan Hardware** option.
2. A device detection operation is performed on the CommCell computers registered to the MediaAgent, and the MediaAgent is updated with the latest hardware setup.

Back to Top

Index Cache

Topics | How To | Troubleshoot | Related Topics

OVERVIEW

The index cache directory is the directory in which index data resides. Each MediaAgent maintains an index cache for the data protection operations performed using that MediaAgent. The index data maintained in the index cache is accessed by the system during data protection, browse, and data recovery operations.

To ensure that other files do not use up disk space that is needed for index data, you can create a partition specifically for the index cache directory. The partition must be large enough to accommodate four percent of the estimated amount of data managed by the MediaAgent.

During the MediaAgent installation, the install program prompts for an index cache location for the specific MediaAgent. This information can be viewed or modified from the **Catalog** tab of the **MediaAgent Properties** dialog box.

- Do not specify or relocate a MediaAgent's index cache to a directory residing on a compressed drive.
- Do not provide the path to the index cache as a folder directly under the Install directory. For example, `\<install folder>\IndexCache`.
- Index cache path supports a maximum of 200 characters. The path cannot contain the special character "!".

GENERATION OF INDEXES

Indexes are generated and maintained at the job level in the index cache on a MediaAgent. When a full or synthetic full backup is run, a new index file is generated. Indexing information gets appended to the index files in the existing index cache with each subsequent incremental backup (from the last job in the cycle). Later the existing index folder gets pruned.

INDEX CACHE PLANNING GUIDE

The Index Cache Directory requires following suggested iOPs specifications. This can be done using IO meter tool which measures the IOPs (Input Output Operations per second). For more information on how to use IoMeter, see IOPs and Capacity Planning Guidelines for Indexing.

MEDIAAGENT CLASS	ESTIMATED DATA BACKED UP PER WEEK (FILE AND E-MAIL DATA)	ESTIMATED INDEX CACHE	RECOMMENDED IOPS
Large	40 - 60 TB	1 TB	400
Medium	20 - 40 TB	500 GB	300
Small	Up to 20 TB	200 GB	250

For best performance and scalability, it is not recommended to host the Index Cache on the CommServe unless your CommServe is your only MediaAgent.

INDEX CACHE RETENTION

Index Cache Retention is the mechanism for retaining and cleaning up index data stored in the Index Cache Directory based on certain rules. This is achieved by specifying appropriate retention rules using the **MediaAgent Properties (Catalog)** tab. Since index cache can grow over a period of time, it is important to specify appropriate Retention Criteria based on which the index folders are retained.

REGULAR CLEANUP

On a regular basis, the index files older than the value set for Index retention time in days are cleaned up once in 24 hours irrespective of disk free percentage. The default value of Index Retention Criteria is 35 days.

You can specify the number of days to retain the index cache using the **Index retention time in days** value in **MediaAgent Properties (Catalog)** tab. The MediaAgent takes care of removing all index files that have not been accessed within the specified number of days.

RETENTION CRITERIA

The amount of index data that can be cached is based on the following parameters:

- **Index Retention Time in days**

  Specifies the number of days for which the index would be retained in the MediaAgent for a specific subclient. Once the number of retention days for a specific index is met, it gets aged once every 24 hours.

- **Index Cleanup Percent**

  It is the disk percentage until which the index cache must be removed after the minimum free space percentage threshold is met. Whenever a backup is initiated, the MediaAgent checks for the available disk space in the disk housing the index cache. If the amount of used disk space exceeds the Minimum Free Space threshold, the MediaAgent removes index files in the index cache on a least recently used basis until the used disk space becomes equal to the Index Cleanup Percent specified here. However, keep in mind that the index retention time will not be taken into consideration during this process.

- **Minimum Free Space (MB)**

  Specifies the total amount of free space that must be available at all times in the index cache. If the **Index Cleanup Percent** is not met, MediaAgent is brought offline and most recent indices are cleaned until **Minimum Free Space** amount is reached.

- **Free Space Warning for Index Cache Using Alerts**

  If the amount of free space falls below the specified amount in the volume in which the Index Cache is stored, the MediaAgent generates an event message and generates the **MediaAgents (Disk Space Low)** alert, if configured. It also starts cleaning up the index based on Least Recently Used (LRU) basis until the free space that specified in **Index cleanup Percent**. See Available Alerts and Alert Descriptions and Space Check Thresholds for the Software Installation and System Directories for detailed information on setting up the alert.

  The above parameters are not applicable for NetWare MediaAgents. Ensure that you have sufficient disk space on the NetWare volume that hosts the index cache before performing data protection operations.

LOCAL INDEX CACHE

A local index cache is maintained in a local path on the MediaAgent computer and can be accessed by that MediaAgent only. The location of the local index cache is configured during the installation of the MediaAgent software.

Local index cache is supported on Windows, Unix, and Netware MediaAgents.

CREATE A LOCAL INDEX CACHE

MediaAgents create the index cache by default, and the location of the index cache is supplied when installing the MediaAgent. Ensure that you have enough space to accommodate the index cache. You might want to estimate the space required using the recommendation specified at Calculating the Storage Space

Required for the Index Cache Directory.

MOVE A LOCAL INDEX CACHE

You can change the location of the index cache and designate a new directory at any time from the **Catalog** tab of the **MediaAgent Properties** dialog box. When you change the directory for index cache, the existing cache contents are moved and all new cache entries are directed to the new location. See Move an Index Cache for step-by-step instructions.

RETENTION

Since index cache can grow over a period of time, you might have to specify the criteria based on which the index cache is retained. See Index Retention Criteria for the available index cache retention settings. See Set the Index Retention Criteria for step-by-step instructions to specify index cache retention.

WHAT IS INDEX CACHE SHARING

The index cache of a MediaAgent can be shared with other MediaAgents. You might want to share the index cache if you wish to define alternate data paths (GridStor) for Storage Policies. When a storage policy uses multiple data paths, then the index cache of all the MediaAgents associated with those data paths must be shared for accessibility reasons. Note that MediaAgents that share the index cache must be of the same release version.

Index cache can be shared using a Index Cache Server or a Network Share.

GUIDELINES FOR CREATING SHARED INDEX CACHE FOR ALTERNATE DATA PATHS (GRIDSTOR)

To create Alternate Data Paths in the CommCell, you must share the index cache so that it can be accessed by all the MediaAgents that are configured with alternate data paths. (See Alternate Data Paths (GridStor) for a detailed description of the topic.)

Follow the guidelines listed below while creating a Shared Index Cache Directory for alternate data paths:

- Ensure that all the MediaAgents that will be configured as data path candidates, point to the same network share and the same folder within this network share for its index cache location.
- If you have both the Unix and Windows MediaAgents pointing to the same folder, make sure that the files and folders are accessible to both these operating systems.
- For MediaAgents that access the Shared Index Cache Directory across domains, make sure that two-way trust relationships between the domains are established.
- If you reboot a Unix MediaAgent, verify and ensure that the mount point to the index cache folder is mounted in same location specified in this **Catalog** tab of the **MediaAgent Properties** dialog box.
- For a Network Shares, if the shared index cache location is changed, then the change must be reflected on all the MediaAgents using the network share.
- For NAS clients, it is required that the Job Results directory resides in a network share that is accessible between the MediaAgents sharing the index cache directory. See Changing the Job Results Path of a Client for steps on changing the directory location.

INDEX CACHE SERVER

Index Cache Server is an index cache sharing mechanism that saves an additional copy of the index cache for sharing purposes. See Index Cache Server for more information on this feature.

NETWORK SHARE

A Network Share is a designated location on the network where one or more MediaAgents store their index cache. The index cache stored in a network share can be accessed all participating MediaAgents. You might use a network share if you have a dedicated partition created exclusively for index cache and you wish to use this partition for index cache sharing.

Ensure that you have enough space to accommodate the index cache from *All* participating MediaAgents. You might want to estimate the space required using the recommendation specified at Calculating the Storage Space Required for the Index Cache Directory.

> **WARNING:**
>
> Note that when using a network share, the local index and the shared index is one and the same. A network disruption might damage the index and jobs might have to be restarted due to index cache failure. So it is recommended that you use Index Cache Server for index cache sharing instead.
>
> It is highly recommended that the option **Enable Intermediate Index Cache Directory** be used when configuring Index Cache on a network share. With this option turned on the index is written to the local disk first and at commit points uploaded to the Network share. This will avoid failures due to network disruptions/failures writing to the index on the network share.

Network Share is supported on Windows and Unix MediaAgents.

When using Network Share with alternate data paths, the **create index** phase of a data protection job, will round-robin between the MediaAgents that share the index. The appropriate MediaAgent's name will be displayed in the **Job Controller** during the **create index** phase of the job.

CREATE A NETWORK SHARE

Use the following procedures to create a shared index cache using Network Share:

1. Create a Network Share profile. See Create a Shared Catalog Profile for step-by-step instructions.
2. Configure the MediaAgents to use the network share to store the index cache. See Configure a MediaAgent for Index Cache Sharing for step-by-step instructions.

MOVE A NETWORK SHARE

You can change the location of the Network Share. When you change the location, the existing cache contents are moved and all new cache entries are directed to the new location. See Move a Shared Index Cache for step-by-step instructions. Note that you will have to change the location on all MediaAgents pointing to the network share.

RETENTION

Retention rules for the index cache entries in a Network Share are specified in the Network Share profile. See Edit a Shared Catalog Server Profile for step-by-step instructions to modify the retention settings.

See Index Retention Criteria for information on index cache retention settings.

CALCULATING THE STORAGE SPACE REQUIRED FOR INDEX CACHE

You need to allocate space for index cache on the local disk of a MediaAgent. The necessary space is typically between 100 GB to 500 GB depending on the amount of total data protected using the MediaAgent.

It is recommended to allot a minimum disk space of 100 GB for intermediate index cache. To calculate the disk space, divide the index cache size by the number of cycles retained in the cache. For example, if the index cache allotted size is 500 GB and retention is 14 days (2 cycles), then you will need 500/2 (= 250) GB for intermediate index cache.

BEST PRACTICES FOR MAINTAINING INDEX CACHE

The following are recommended as best practices for maintaining index cache:

- If possible, use a file system that is dedicated to index cache data only (so that non index data does not grow and encroach on the index cache capacity.
- Use a more liberal than a conservative estimate while allocating space for index cache.
- Make sure to consider the space allocated for index cache in the following cases:

  When clients are added to a MediaAgent.

  When the backup cycle is modified.

  Factors that affect the composition of backups, such as the data size, file names, etc.
- If you are maintaining backward-compatible content indexes generated by a previous software version, additional disk space may be required in the index cache folder. For information, see *Books Online* of the previous software version.

INDEX CHECK POINTING

Index Check Pointing option, which provided job restartability in failover scenarios, is a deprecated feature in this release. On upgraded clients, if you have been using the index check pointing feature in the previous release, then you might continue to see the option in the **Advanced Backup Options - Data** tab. We strongly recommend that you disable this option and use Catalog Server with transaction logging feature instead. For more information on using this feature, see Using Index Cache Server for Job Restarts in Failover Scenarios

UPGRADE CONSIDERATIONS

MediaAgents participating in index cache sharing must operate in the same version. When the Index Cache of a MediaAgent is shared, then all MediaAgents participating in the share must be upgraded together.

RELATED REPORT

The CommCell Configuration Report provides the following information on index cache disk usage for each MediaAgent in the CommCell. This information is useful to identify index cache growth and manage the disk space accordingly.

- Total amount of space available in the index cache location.
- Amount of space used by index cache entries.

See CommCell Configuration Report for information on how to use the report.

AUDIT TRAIL

Operations performed with this feature are recorded in the Audit Trail. See Audit Trail for more information.

Back To Top

Index Cache - How To

Topics | How To | Troubleshoot | Related Topics

CREATE A NETWORK SHARE PROFILE

Required Capability: Capabilities and Permitted Actions

To create a network share profile for index cache sharing:

1. From the CommCell Browser, right-click the CommServe, click **Control Panel,** and select **Shared Catalog Configuration**.

   Alternatively, from the CommCell Browser, right-click the MediaAgent, and click **Configure.**
2. From the Shared catalog Configuration dialog box, click **Add** to create a Network Share Profile.
3. Enter the name of the Profile to be created in **Profile Name** box.
4. Select the type of index share:
   - **Network Share** - Network share directs the index cache to a common network location.
5. In the **Profile Properties** area, specify the following retention criteria for the shared index cache.
   - **Index Retention Time in days** - Select the number of days after which an index cache can be removed. This criteria is used for the purpose of removing index cache.
   - **Index Cleanup Percent** - Select the disk percentage used to remove the index cache.
   - **Minimum Free Space (MB)** – Select the total amount of free space that must be available at all times in the index cache.
   - **Free Space Warning (MB)** – Select the amount of free space in the index cache. If the amount of free space falls below the specified amount, the

MediaAgent generates an event message and generates the MediaAgents (Disk Space Low) alert, if configured.

6. Click **OK** to create the profile. You can use this profile on a MediaAgent to share the index cache.

CONFIGURE A MEDIAAGENT FOR INDEX CACHE SHARING

Required Capability: Capabilities and Permitted Actions

➤ To configure a MediaAgent for index cache sharing:

1. From the CommCell Browser, right-click the MediaAgent you wish to share the index cache and click **Properties**.
2. From the **MediaAgent Properties** window click the Catalog tab.
3. Select **Catalog Profile** option to enable index cache sharing.
4. To use a Network Share, click **Network Share** and select a Network Share profile from the list. All **Network Share** profiles created from the **Shared Catalog Configuration** window will be available for selection.

   Point your index cache to the network share location.

   For Windows MediaAgents:

   - Select **Use Network Share** - if the index cache will reside on a network share.
   - In the **Index Cache Directory** box, type the path to the index cache directory or use the **Browse** button to select the path.
   - Click the **Change** button. In the Change User Account dialog box, type the user account and password that must be used to access the Index Cache and then click **OK**.
   - It is highly recommended that the option **Enable Intermediate Index Cache Directory** be used when configuring Index Cache on a network share. With this option turned on the index is written to the local disk first and at commit points uploaded to the Network share. This will avoid failures due to network disruptions/failures writing to the index on the network share.
   - Click **OK** to save the configuration.

   For Unix MediaAgents:

   - In the **Index Cache Directory** box, type the path to the index cache directory or use the **Browse** button to select the path. If the index cache resides on a network share, then this will be the path to network index cache mounted locally.
   - It is highly recommended that the option **Enable Intermediate Index Cache Directory** be used when configuring Index Cache on a network share. With this option turned on the index is written to the local disk first and at commit points uploaded to the Network share. This will avoid failures due to network disruptions/failures writing to the index on the network share.
   - Click **OK** to save the configuration.
5. The index cache is shared.
6. Now this index is available to be shared from other MediaAgents.
7. Right-click *another MediaAgent* that will share the index and then click **Properties**.
8. Click the the Catalog tab.
9. Select **Catalog Profile** option to enable index cache sharing.
10. To use a Network Share, click **Network Share** and select a Network Share profile from the list. All **Network Share** profiles created from the **Shared Catalog Configuration** window will be available for selection.

    Point your index cache to the network share location.

    For Windows MediaAgents:

    - Select **Use Network Share** - if the index cache will reside on a network share.
    - **Use MediaAgent Local Drive** - if the index cache will reside on a local drive.
    - In the **Index Cache Directory** box, type the path to the index cache directory or use the **Browse** button to select the path.
    - Click the **Change** button. In the Change User Account dialog box, type the user account and password that must be used to access the Index Cache and then click **OK**.
    - It is highly recommended that the option **Enable Intermediate Index Cache Directory** be used when configuring Index Cache on a network share. With this option turned on the index is written to the local disk first and at commit points uploaded to the Network share. This will avoid failures due to network disruptions/failures writing to the index on the network share.
    - Click **OK** to save the configuration.

    For Unix MediaAgents:

- In the **Index Cache Directory** box, type the path to the index cache directory or use the **Browse** button to select the path. If the index cache resides on a network share, then this will be the path to network index cache mounted locally.
- Click **OK** to save the configuration.

11. Repeat steps 8 -10 on all the MediaAgents that share the index cache.

ENABLE (OR DISABLE) INDEX CACHE SHARING FOR A JOB

Before You Begin

The catalog server option for the job is applicable only if the MediaAgent performing the backup is configured for index cache sharing.

Required Capability: Capabilities and Permitted Actions

➡ To enable (or disable) index cache sharing using catalog server:

1. From the CommCell Browser, select one of the following:
   - To backup a subclient, right-click the subclient to want to backup and click **Backup**.
   - To backup a user-defined backup set or instance, right-click the backup set you want to backup, click **All Tasks**, and click **Backup All Subclients**.
   - To backup the default backup set, right-click the agent or instance node, click **All Tasks**, and click **Backup Default Backup Set**.
   - For Lotus Notes *i*DataAgent, to backup a partition, right-click the partition you want to backup, click **All Tasks**, and click **Backup Default Backup Set**.
   - For Agents that do not have backup set or instance levels, to backup all subclients, right-click the agent icon, click **All Tasks**, and click **Backup All Subclients**.
2. If you chose a level higher than subclient (i.e., backup set, etc.), you are prompted to confirm that you want to back up all the subclients below that level. Click **Yes**.
3. If you want to adjust the granular restartability option for the backup job, click **Advanced** from the **Backup Options** window.

   From the **Advanced Backup Options (Data)** tab, select one of the following options.
   - **Use shared profile if present with transaction logging** for index cache sharing along with the transaction logging feature for granular job restartability. This option is enabled by default and recommended for all configurations.
   - **Use shared profile if present without transaction logging** for index cache sharing without the transaction logging feature. This option reduces the network traffic between the MediaAgent and the Index Cache Server by limiting the amount of data being transferred. This configuration is not recommended because if a job fails or gets restarted, it will start from the beginning.
   - **Use Transaction logging** for the granular job restartability feature. This option is designed for a standalone MediaAgent without an Index Cache Server as it allows the job to restart from the last commit point in the case of a power failure, system error or another unexpected job termination.
   - **None** to disable index cache sharing. When selected, the index cache is stored in the MediaAgent's local index cache only.
4. Click **OK.**

DELETE A NETWORK SHARE PROFILE

Required Capability: Capabilities and Permitted Actions

➡ To delete a catalog server profile:

1. From the CommCell Browser, right-click the CommServe, click **Control Panel,** and select **Shared Catalog Configuration**.
2. From the Shared catalog Configuration dialog box, click **Delete** to delete a Network Share Profile. A confirmation message is displayed. Click **OK** to delete the Network Share Profile.
3. Click **OK** to save changes in the shared catalog Configuration and close the dialog box.

EDIT A NETWORK SHARE PROFILE

Required Capability: Capabilities and Permitted Actions

➡ To edit a network share profile:

1. From the CommCell Browser, right-click the CommServe, click **Control Panel,** and select **Shared Catalog Configuration**.

   Alternatively, from the CommCell Browser, right-click the MediaAgent, and click **Configure.**
2. From the Shared catalog Configuration dialog box, select the profile you wish to edit and click **Edit**. The Shared Catalog Configuration window is displayed.
3. Change the name of the profile in the **Profile Name** box.

4. You can change the following retention parameters:
   - Index retention time in days
   - Index cleanup percent
   - Minimum Free Space in MB
   - Free Space Warning in MB
5. Click **OK** to save the configuration.

SET THE INDEX RETENTION CRITERIA FOR NETWORK SHARE PROFILES

Required Capability: Capabilities and Permitted Actions

➡ To establish the index retention criteria for network share profiles:

1. From the CommCell Browser, click the **MediaAgents** icon. All the MediaAgents available in the CommCell are displayed on the right-pane of the CommCell Browser.
2. Right-click the MediaAgent whose index cache parameters you wish to modify, and then click **Properties**.
3. Click the Catalog tab of **MediaAgent Properties** dialog box.
4. You can change the following retention parameters:
   - Index retention time in days
   - Index cleanup percent
   - Minimum Free Space in MB
   - Free Space Warning in MB
5. Click **OK** to save the configuration.

MOVE AN INDEX CACHE

Before You Begin

- For Unix MediaAgents, if the index cache resides on a network share, you have to manually mount the drive containing the index cache to the local machine to be able to create a shared index cache. Also note down the local mount path.

Required Capability: Capabilities and Permitted Actions

➡ To move an index cache:

1. From the CommCell Browser, right-click the MediaAgent for which you wish to move the index cache and then click **Properties**.
2. Click the Catalog tab.
3. Provide details in the **Index Cache** area.

   For Windows MediaAgents:

   - Select **Use Network Share** if the index cache will reside on a network share, and select **Use MediaAgent Local Drive** if the index cache will reside on a local drive.
   - In the **Index Cache Directory** box, type the path to the index cache directory or use the **Browse** button to select the path.
   - If the MediaAgent resides on a Network Share, click the **Change** button. In the Change User Account dialog box, type the user account and password that must be used to access the index cache and then click **OK**.

   For Unix MediaAgents:

   - In the **Index Cache Directory** box, type the path to the index cache directory or use the **Browse** button to select the path. If the index cache resides on a network share, then this will be the path to network index cache mounted locally.
4. Click **OK** to save the configuration.
5. If the index is moved from a local drive to a network share, a **Confirm** prompt is displayed, asking you whether you wish to copy the index cache. Click one of the following:
   - **Yes** to copy the index cache to the new index cache folder.
   - **No** to move the index cache without copying the index cache folder. In this case subsequent jobs may result in index restore operation from the media.
6. The index cache is moved to the new folder.

NOTES

- It is important that you do not change the Name of the Profile when moving a shared index cache.
- On Windows MediaAgents, the original directory may have to be manually deleted to free the disk space.
- Index Cache can only be moved when no index jobs like Auxiliary Copy, Disaster Recovery Backups, Deduplication Backups, etc. are running.
- If you wish to manually move the index cache, see Manually Relocate the Index Cache.
- If the index cache contains SnapProtect backup data, you will have to Manually Relocate the Index Cache.

MOVE A SHARED INDEX CACHE

Before You Begin

- For unix MediaAgents, if the index cache resides on a network share, you have to manually mount the drive containing the index cache to the local machine to be able to create a shared index cache. Also note down the local mount path.

Required Capability: Capabilities and Permitted Actions

To move a shared index cache:

1. From the CommCell Browser, right-click *any one* of the MediaAgents that share the shared index cache and then click **Properties**.
2. Click the Catalog tab.

   For Windows MediaAgents:

   - Select **Use Network Share** if the index cache will reside on a network share, and select **Use MediaAgent Local Drive** if the index cache will reside on a local drive.
   - In the **Index Cache Directory** box, type the path to the index cache directory or use the **Browse** button to select the path.
   - If the MediaAgent resides on a Network Share, click the **Change** button. In the Change User Account dialog box, type the user account and password that must be used to access the Index Cache and then click **OK**.

   For Unix MediaAgents:

   - In the **Index Cache Directory** box, type the path to the index cache directory or use the **Browse** button to select the path. If the index cache resides on a network share, then this will be the path to network index cache mounted locally.
3. Click **OK** to save the configuration.
4. Repeat the above steps *on all* the MediaAgents that share the index cache. If this is not done, the index cache will be turned offline after 30 minutes, and all the jobs accessing the MediaAgents that share this index cache may fail as a result.

NOTES

- It is important that you do NOT change the **Name** of the Network Profile when moving a shared index cache.
- On Windows MediaAgents, the original directory may have to be manually deleted to free the disk space.
- Index Cache can only be moved when no index jobs like Auxiliary Copy, Disaster Recovery Backups, Deduplication Backups, etc. are running.

MANUALLY RELOCATE THE INDEX CACHE

The Index Cache can be moved from the CommCell Console, as described in Move an Index Cache. But in some situations it might be necessary to manually relocate the index cache. For example, if the index cache folder is too large, MediaAgent install folder needs to be moved, etc. Use the following procedure in such situations.

Before You Begin

- For unix MediaAgents, if the index cache resides on a network share, you have to manually mount the drive containing the index cache to the local machine to be able to create a shared index cache. Also note down the local mount path.

Required Capability: Capabilities and Permitted Actions

To manually relocate an index cache:

1. Copy the Index Cache to the desired location.
2. Navigate to this location and delete the `icl_label.txt` file.
3. From the CommCell Browser, right-click the MediaAgent for which you wish to move the index cache and then click **Properties**.
4. Click the Catalog tab.
5. Provide details in the **Index Cache** area.

   For Windows MediaAgents:

- Select **Use Network Share** if the index cache will reside on a network share, or select **Use MediaAgent Local Drive** if the index cache will reside on a local drive.
- In the **Index Cache Directory** box, type the path to the index cache directory or use the **Browse** button to select the path.
- If the MediaAgent resides on a Network Share, click the **Change** button. In the Change User Account dialog box, type the user account and password that must be used to access the Index Cache and then click **OK**.

For Unix MediaAgents:

- In the **Index Cache Directory** box, type the path to the index cache directory or use the **Browse** button to select the path. If the index cache resides on a network share, then this will be the path to network index cache mounted locally.

6. Click **OK** to save the configuration.
7. Click **NO** in the **Confirm** prompt.

   The index cache is relocated to the new folder.

UNSHARE A SHARED INDEX CACHE

Before You Begin

- Ensure that the MediaAgent is not defined as an alternate data path candidate in any of the storage policy copies. If the MediaAgent is used as candidate, the system will automatically prevent you from unsharing the index cache.
- For Unix MediaAgents, if the index cache resides on a network share, you have to manually mount the drive containing the index cache to the local machine to be able to create a shared index cache. Also note down the local mount path.

Required Capability: Capabilities and Permitted Actions

To unshared a shared index cache:

1. From the CommCell Browser, right-click the MediaAgent for which you wish to unshare the shared index cache and then click **Properties**.
2. From the Catalog tab, uncheck the **Catalog Profile** option. The index cache is no longer shared.
3. If you were using a Network Share, then you will have to provide a local path for the index cache. Perform one of the following:

   For Windows MediaAgents:

   - Select **Use Network Share** if the index cache will reside on a network share, or select **Use MediaAgent Local Drive** if the index cache will reside on a local drive.
   - In the **Index Cache Directory** box, type the path to the index cache directory or use the **Browse** button to select the path.
   - If the MediaAgent resides on a Network Share, click the **Change** button. In the Change User Account dialog box, type the user account and password that must be used to access the Index Cache and then click **OK**.

   For Unix MediaAgents:

   - In the **Index Cache Directory** box, type the path to the index cache directory or use the **Browse** button to select the path. If the index cache resides on a network share, then this will be the path to network index cache mounted locally.
4. Click **OK** to save the configuration.

INTERMEDIATE INDEX CACHE

You can use **Intermediate Index Cache Directory** when configuring Index Cache on a network share. With this option turned on the index is written to the local disk first and at commit points uploaded to the Network share. This will avoid failures due to network disruptions/failures writing to the index on the network share. This can be done for both Windows and Unix MediaAgents.

WINDOWS MEDIAAGENTS

1. In the CommCell browser, expand Storage Resources and then navigate to MediaAgents.
2. Right-click the MediaAgent you wish to share and click **Properties**.
3. From the **MediaAgent Properties** window click the Catalog tab.
4. Select the **Catalog Profile** option and click **Network Share.**
5. Select a Network Share profile from the list.

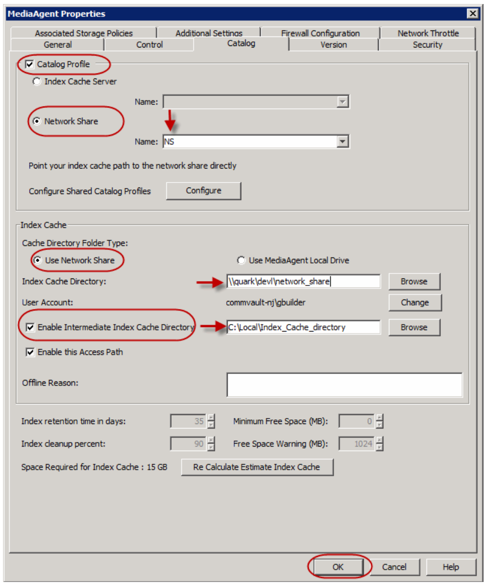
   All Network Share profiles created from the Shared Catalog Configuration window will be available for selection.

6. Select **Use Network Share** and in the **Index Cache Directory** box, type the path to the index cache directory.

   You may alternatively use the **Browse** button to select the path.

7. Click the **Change** button. In the Change User Account dialog box, type the user account and password that must be used to access the Index Cache and then click **OK**.
8. Select **Enable Intermediate Index Cache Directory** and type the path to the index cache directory or use the **Browse** button to select the path.
9. Click **OK** to save the configuration.

   The index cache is shared.



MediaAgent Properties

☑ Catalog Profile

○ Index Cache Server

Name:

● Network Share

Name: NS

Point your index cache path to the network share directly

Configure Shared Catalog Profiles

Index Cache

Cache Directory Folder Type:

● Use Network Share ○ Use MediaAgent Local Drive

Index Cache Directory: \\quark\devl\network_share

User Account: commvault-nj\gbuilder

☑ Enable Intermediate Index Cache Directory: C:\Local\Index_Cache_directory

☑ Enable this Access Path

Offline Reason:

Index retention time in days: 35

Minimum Free Space (MB): 0

Index cleanup percent: 90

Free Space Warning (MB): 1024

Space Required for Index Cache : 15 GB

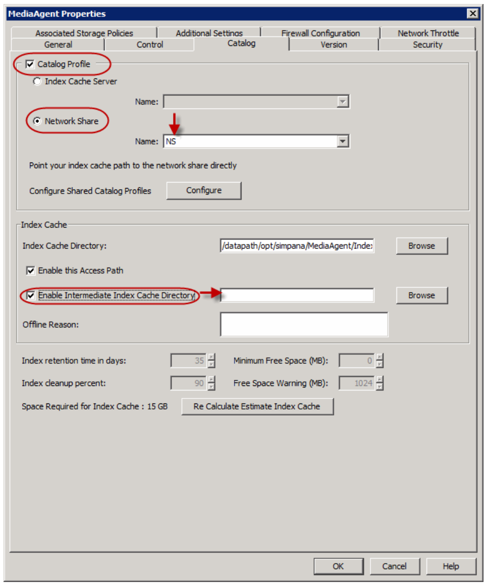
UNIX MEDIAAGENTS

1. In the CommCell browser, expand Storage Resources and then navigate to MediaAgents.
2. Right-click the MediaAgent you wish to share and click **Properties**.
3. From the **MediaAgent Properties** window click the Catalog tab.
4. Select the **Catalog Profile** option and click **Network Share.**
5. Select a Network Share profile from the list.

   All Network Share profiles created from the Shared Catalog Configuration window will be available for selection.

6. Select **Enable Intermediate Index Cache Directory** and type the path to the index cache directory or use the **Browse** button to select the path.
7. Click **OK** to save the configuration.

   The index cache is shared.



MediaAgent Properties

☑ Catalog Profile

○ Index Cache Server

Name:

● Network Share

Name: NS

Point your index cache path to the network share directly

Configure Shared Catalog Profiles

Index Cache

Index Cache Directory: /datapath/opt/simpana/MediaAgent/Inde:

☑ Enable this Access Path

☑ Enable Intermediate Index Cache Directory

Offline Reason:

Index retention time in days: 35

Minimum Free Space (MB): 0

Index cleanup percent: 90

Free Space Warning (MB): 1024

Space Required for Index Cache : 15 GB

Library Operations

Topics | How To | Troubleshoot | Related Topics

OVERVIEW

The following sections describe the various library operations that can be performed from the CommCell Console. The chapter organization follows the order in which these operations are displayed in the CommCell Console. Keep in mind that a general set of library operations are listed in this chapter. These operation are applicable for tape or optical libraries with barcode readers which are configured as direct-attached libraries, direct-attached shared libraries or libraries configured in a SAN environment. Some of these operations may not be applicable for other types of libraries, such as libraries without barcode readers (blind libraries), stand-alone drives, etc. For specific information on other libraries, refer to the following topics:

- Blind Libraries
- Direct-Attached Libraries
- Direct-Attached Shared Libraries
- IP Libraries (Like libraries attached to ACSLS Server)
- NAS Library and Drive Configuration
- Optical Libraries
- PnP (Plug and Play) Disk Libraries
- SAN-Attached Libraries
- Stand-Alone Drives

EXPORT MEDIA

Exporting is the process by which you physically remove one or more media from a library.

For comprehensive information on exporting media, see Export Media.

IMPORT MEDIA

Importing is the process by which you move media that are outside a library into storage slots within the library.

For comprehensive information on importing media, see, Import Media.

IMPORT CLEANING MEDIA

When you import a cleaning media, the system automatically assigns it to the cleaning media pool. For comprehensive information on cleaning media, see Cleaning Media.

DISCOVER MEDIA

Before using a new media, the MediaAgent software must collect certain information about it through a process known as discovery.

For comprehensive information on discovering media, see Discover Media.

Back to Top

DISCOVER CLEANING MEDIA

When you discover cleaning media, the system automatically assigns it to the `Cleaning Media` pool.

For comprehensive information on discovering media, see Discover Media.

For comprehensive information on cleaning media, see Cleaning Media.

SET MEDIA LOCATION

This option allows you to define media locations in bulk.

For comprehensive information ,see Set Media Location.

RESET LIBRARY

You can use the Reset command when you wish to unmount all the media mounted in the drives, and reset all the drives so that they are ready for use.

For comprehensive information on Resetting a library see Reset Library.

MARK LIBRARY FIXED

Use the `Mark Library Fixed` option, to reset the counters that keep track of library events and bring the library online.

See Library Maintenance Threshold Parameters for information on setting up the threshold values for the library.

For comprehensive information on Marking a Library as Fixed see Mark Library Fixed.

MARK MEDIA EXPORTED

Use this feature to mark all the media in a library or in all the libraries as exported.

For comprehensive information on exporting media, see Export Media.

UPDATE BARCODES

The ability to update barcodes associated with the media ensures that the data available in the media is accessible.

For comprehensive information on updating barcodes, see Update Media Barcodes.

When this operation is performed at the library level, all the barcodes associated with media in the library is modified. Barcodes associated with the individual media can also be modified by selecting the specific media from the appropriate Media Group in the library.

FULL SCAN

Full Scan operation identifies the slot location and barcode or media identifier of every media detected within the library.

For comprehensive information on Full Scan Operation, see Full Scan.

Clean Drive

Use this option to concurrently start the clean drives operation on several drives. For a detailed discussion on this option and drive cleaning in general, see Drive Cleaning. You can also start the clean drive operation for a specific drive from the drive level.

Erase Spare Media

The erase spare media operation ensures that old data from removable media (tapes and optical platters) are not recoverable once the media is recycled.

For comprehensive information on erasing spare media, see Erase Spare Media.

Audit Trail

Operations performed with this feature are recorded in the Audit Trail. See Audit Trail for more information.

Related Alerts

The following Media Management Library Management alerts can be configured from the Alerts Wizard:

- Insufficient Storage
- Maintenance Occurred
- Maintenance Required
- Media Handling Required
- Media Mount and Usage Errors
- User Overwrite of Media
- Media Ready in Mail Slot
- Media Recalled

For more information, see:

- Alerts: Media Management
- Configure Alerts

Back To Top

Library Operations - How To

Topics | How To | Troubleshoot | Related Topics

Move a Library to Another MediaAgent Without Data Loss

In some situations you may have the need to move a library from one MediaAgent to another due to re-configuration or other requirements.

The following procedure provides step-by-step instructions on how to perform this operation.

1. Detach the library and attach it to the new MediaAgent and make sure that the hardware is visible to the operating system. See Driver Configurations for more information.
2. Open the CommCell Console and change the name of the MediaAgent associated with the library. See Change the MediaAgent (Host) Associated with a Library for more information.

3. If necessary run a quick backup to verify that the devices are functioning correctly.

CHANGE THE MEDIAAGENT (HOST) ASSOCIATED WITH A LIBRARY

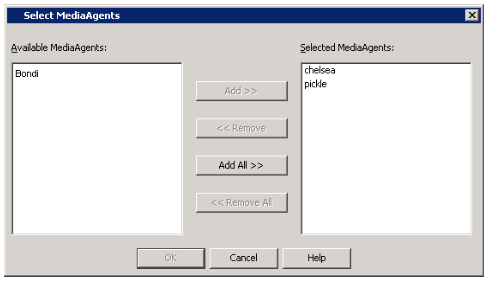
The following procedure outlines the steps involved in changing the MediaAgent associated with a library. Use this procedure when you attach the library to a different MediaAgent

TO CHANGE THE MEDIAAGENT ASSOCIATED WITH A LIBRARY

1. Detach the library from the old MediaAgent computer and attach it to the new MediaAgent computer.
2. Check and verify that the library and drives are visible to the operating system in the new MediaAgent computer.

   For a more detailed explanation on verifying the driver configurations, see Driver Configurations.
3. Display the Library and Drive Configuration window.

   Select only the old and new MediaAgents in the **Select MediaAgents** dialog box.



Select MediaAgents

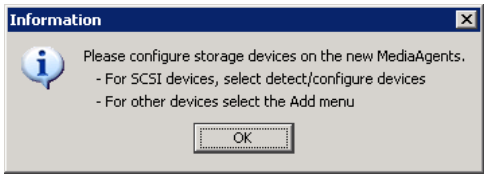
Available MediaAgents: Bondi

Selected MediaAgents: chelsea, pickle

4. Click **OK** in the Information prompt.

   This prompt is displayed as the library is not yet configured in the new MediaAgent.

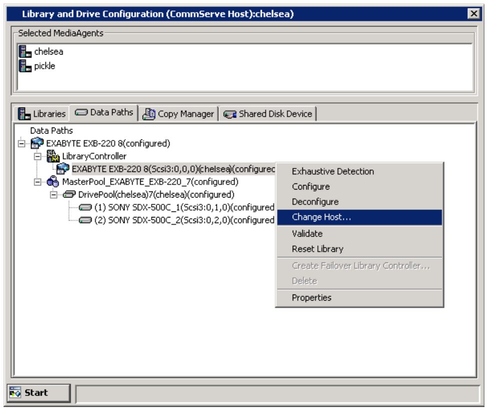
   The system displays the library configured under the old MediaAgent.



Information

Please configure storage devices on the new MediaAgents.
- For SCSI devices, select detect/configure devices
- For other devices select the Add menu

5. Right-Click the library controller and then choose **Change Host**.

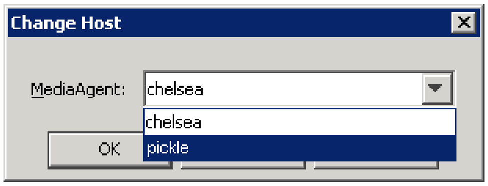


Library and Drive Configuration (CommServe Host):chelsea)

Selected MediaAgents: chelsea, pickle

Data Paths
EXABYTE EXB-220 8(configured)
LibraryController
EXABYTE EXB-220 8(Scsi3:0,0,0)(chelsea)(configurec
MasterPool_EXABYTE_EXB-220_7(configured)
DrivePool(chelsea)7(chelsea)(configured)
(1) SONY SDX-500C_1(Scsi3:0,1,0)(configured
(2) SONY SDX-500C_2(Scsi3:0,2,0)(configured

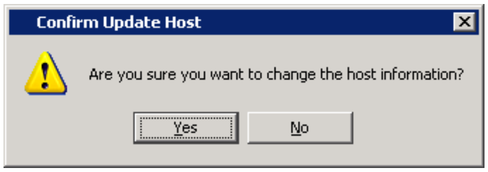
6. Select the name of the new MediaAgent to which the library is currently attached.



Change Host

MediaAgent: chelsea

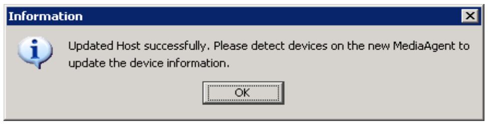
7. Click **Yes** in the confirm prompt.



Confirm Update Host

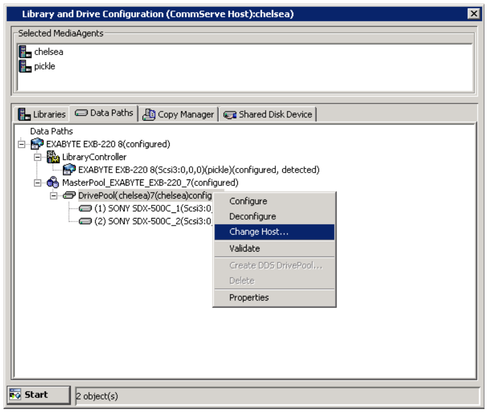
Are you sure you want to change the host information?

8. Click **OK** in the Information prompt.

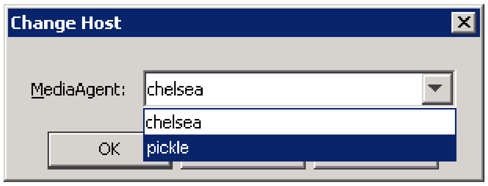


Updated Host successfully. Please detect devices on the new MediaAgent to update the device information.

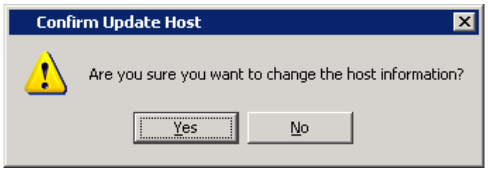
9. Right-click the **DrivePool** and then choose **Change Host**.


Library and Drive Configuration (CommServe Host):chelsea)
Selected MediaAgents
chelsea
pickle
Libraries
Data Paths
Copy Manager
Shared Disk Device
Data Paths
EXABYTE EXB-220 8(configured)
LibraryController
EXABYTE EXB-220 8(Scsi3:0,0,0)(pickle)(configured, detected)
MasterPool_EXABYTE_EXB-220_7(configured)
DrivePool(chelsea)7(chelsea)config
(1) SONY SDX-500C_1(Scsi3:0
(2) SONY SDX-500C_2(Scsi3:0
Configure
Deconfigure
Change Host...
Validate
Create DDS DrivePool...
Delete
Properties
Start
2 object(s)

10. Select the name of the new MediaAgent to which the library is currently attached.

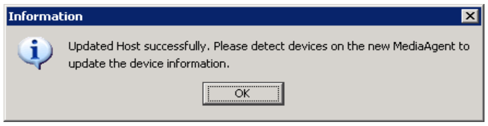


11. Click **Yes** in the confirm prompt.



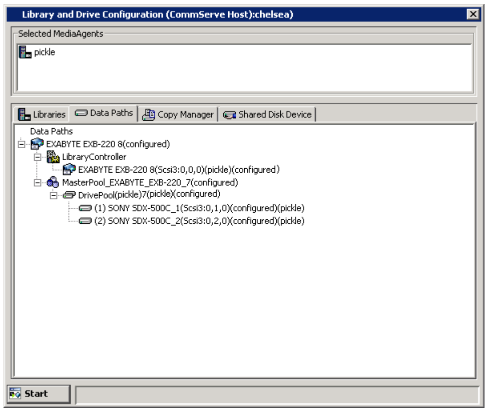
Are you sure you want to change the host information?

12. Click **OK** in the Information prompt.



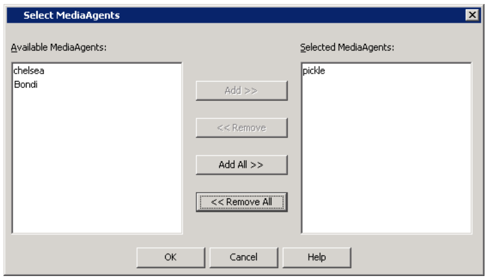
Updated Host successfully. Please detect devices on the new MediaAgent to update the device information.

The system displays the library configured under the new MediaAgent.


Library and Drive Configuration (CommServe Host):chelsea)
Selected MediaAgents
pickle
Libraries
Data Paths
Copy Manager
Shared Disk Device
Data Paths
EXABYTE EXB-220 8(configured)
LibraryController
EXABYTE EXB-220 8(Scsi3:0,0,0)(pickle)(configured)
MasterPool_EXABYTE_EXB-220_7(configured)
DrivePool(pickle)7(pickle)(configured)
(1) SONY SDX-500C_1(Scsi3:0,1,0)(configured)(pickle)
(2) SONY SDX-500C_2(Scsi3:0,2,0)(configured)(pickle)
Start

13. From the **Start** Menu, click **Select MediaAgents**.

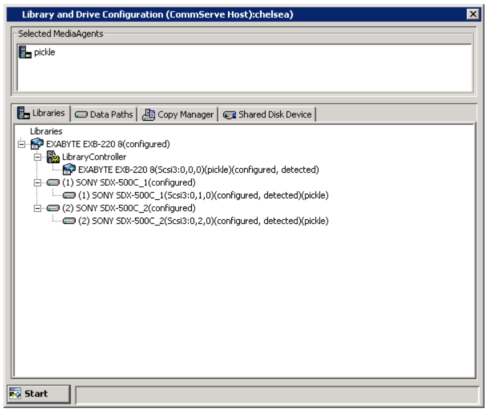
In the **Select MediaAgents** dialog box, select the name of the MediaAgent to which the library is currently attached.



14. Detect the devices as described in Detect Devices.

Once the detection process is complete, the devices should be displayed with `configured, detected` status.

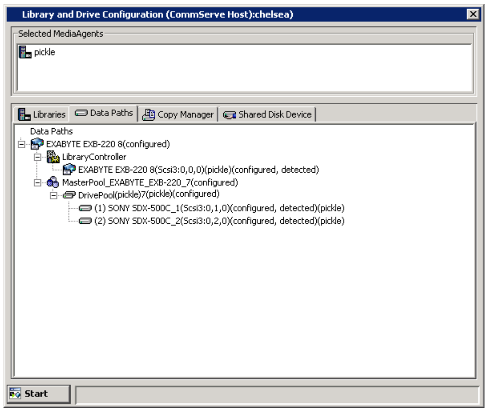
The **Library** tab provides the physical view of the devices (library and drives).



```
pickle
```

```
Libraries
⊟ EXABYTE EXB-220 8(configured)
    ⊟ LibraryController
        EXABYTE EXB-220 8(Scsi3:0,0,0)(pickle)(configured, detected)
    ⊟ (1) SONY SDX-500C_1(configured)
        (1) SONY SDX-500C_1(Scsi3:0,1,0)(configured, detected)(pickle)
    ⊟ (2) SONY SDX-500C_2(configured)
        (2) SONY SDX-500C_2(Scsi3:0,2,0)(configured, detected)(pickle)
```

The **Data Paths** tab provides a logical view of the data path used to access the devices - library, master drive pool, drive pool, drive.



```
pickle
```

```
Data Paths
⊟ EXABYTE EXB-220 8(configured)
    ⊟ LibraryController
        EXABYTE EXB-220 8(Scsi3:0,0,0)(pickle)(configured, detected)
    ⊟ MasterPool_EXABYTE_EXB-220_7(configured)
        ⊟ DrivePool(pickle)7(pickle)(configured)
            (1) SONY SDX-500C_1(Scsi3:0,1,0)(configured, detected)(pickle)
            (2) SONY SDX-500C_2(Scsi3:0,2,0)(configured, detected)(pickle)
```

Reuse Media with Failed Content Verification

Required Capability: See Capabilities and Permitted Actions

Use the following procedure to overwrite media in situations where the MediaAgent fails to read a media, e.g., incompatible data formats, etc.

To reuse media with failed content verification:

1. From the CommCell Browser, right-click the library for which you wish to reuse media with failed content verification, and then click **Properties**.
2. Click the Media tab.
3. From the **Overwrite Media** region, click **When Content Verification Failed.**
4. Click **OK** to save the changes.

Export Media

Topics | How To | How Do I | Related Topics

OVERVIEW

Exporting is the process by which you physically remove one or more media from a library. If a data protection operation requests an exported media, depending on the options selected for the library in the Media tab of the **Library Properties** dialog box, one of the following operation will be performed:

- The exported media will be automatically marked as **full**, and a new media will be used for the data protection operation.
- The job will remain in the **waiting** state, with the **Reason for job delay** stating that the media is outside the library.

However, if a restore or auxiliary copy job requires data from an exported media, the system will prompt you to import the media in order to complete the operation. Information about exported media will be retained in the system; they do not have to be rediscovered if they are re-imported.

> If a media is reserved by a job for a read or write operation, the media cannot be exported.

When a media is exported an optional entry to specify the storage location for the media is provided. This information, can be viewed or updated in the **Media Properties** dialog box. This feature helps you to keep track of the exported media. The exported media are displayed with the location in the **Exported Media** pool in the CommCell Console.

> Media that is left in the mail slot after an export operation will be treated as an exported media. Pop-up messages associated with media outside the library and the media information in the CommCell Console will indicate that the media is in the IEPort associated with the mail slot.
> You can use VaultTracker and Media Repository in VaultTracker to manage media residing outside the library.

There are two ways to remove the media from the library:

- You can remove the media through the library's mail slot (if available and supported by the library).
- You can open the library door and remove media from the storage slots by hand.

Removing media through a mail slot offers the following advantage: The inventory update that is triggered by a mail slot export is much less time-consuming than the full inventory operation that is triggered when you close the library door. However, under certain circumstances you may want to open the library door even though a mail slot is available. For example, if you want to remove many media from a library at once, it may be faster to open the door than to use the mail slot.

> Removing media from and closing the mail slots of some libraries may trigger a full inventory operation (rather than an inventory update).

When the mail slot is full, the system retries the export operation and the number of retries is based on the **Export Operation Retry Count** option in the Media Management Configuration (Service Configuration) dialog box available in the **Control Panel**.

Information about exported media can be obtained from the following:

- Admin Job History

- Media Information Report
- Tracking Report

In addition, you can also use the Media Information Report to obtain a list of media that can be exported.

Media can be exported in several ways:

- Export a specific Media
- Export several media from a list
- Export media using VaultTracker

These are explained in detail in the following sections.

HOW TO EXPORT MEDIA

There are four ways to export media from a library to an outside location depending on the needs of your organization:

- The Export Media Wizard, which provides the capability to quickly select any number of available media for export.
- The Export a Specific Media option allows you to immediately export a specific media if you know the media is available in the library.
- The Export Media From a List option allows you to immediately export several media at the same time if you know either the media's barcode or slot number in which the media resides.
- You can also Export Media Using VaultTracker. This option is useful if you wish to export media based on criteria and/or you wish to schedule the export media operation. VaultTracker also allows you to create VaultTracker alerts, generate VaultTracker reports, assign virtual mail slots, and record pending actions, which are useful in monitoring media movement.

EXPORT MEDIA USING THE EXPORT MEDIA WIZARD

The **Export Media Wizard** provides the capability to quickly export one or more media from a library. This wizard is useful if you know the library containing the media you wish to export, as well as the media to be exported. You can choose to export media in 2 ways:

- using the VaultTracker/VaultTracker Enterprise feature, which provides all the options you need create tracking policies.
- from a list of available media in the library, from which you can select the appropriate media to be exported. The media will then be automatically placed in the appropriate mail slot for removal.

The Export Media Wizard is accessible at the **Library** and **Media in Library** levels in the CommCell Console. See Export Media using the Export Media Wizard for step-by-step instructions.

See Exporting Media using VaultTracker and VaultTracker Enterprise for more information on exporting media using VaultTracker and VaultTracker Enterprise.

EXPORT A SPECIFIC MEDIA

If you wish to export only one specific media, and know where the media is available in the library, you can use this option. A specific media can be exported from the following levels in the CommCell Console:

- Media in Library (discovered and undiscovered media)
- Scratch pools
- Cleaning Media
- Retired Media
- Assigned Media
- **Media List** dialog box which appears when you select the **View Media** option. This dialog box can be accessed by right-clicking a Storage Policy copy.
- **Media List** dialog box which appears when you select the **Change Data Path** option. This dialog box can be accessed by right-clicking a Storage Policy copy.
- **Media List** dialog box which appears when you select the **Media Not Copied** option. This dialog box can be accessed by right-clicking a Storage Policy and Storage Policy copy.
- **Media Used By Job ID** dialog box which appears when you select the **View Media** option from the **Data Protection Job history**, **Backup Job History**, or **Data Migration** windows.

See Export a Specific Media for step-by-step instructions.

EXPORT MEDIA FROM A LIST

Media can be selected from a list of media and exported. This is useful when you wish to export several media at the same time and know either the media's barcode, or slot number in which the media resides. This task can be performed from the following levels in the CommCell® Console:

- **Media List** dialog box which appears when you select the **View Media** option. This dialog box can be accessed by right-clicking a Storage Policy copy.
- **Media List** dialog box which appears when you select the **Change Data Path** option. This dialog box can be accessed by right-clicking a Storage Policy copy.
- **Media List** dialog box which appears when you select the **Media Not Copied** option. This dialog box can be accessed by right-clicking a Storage Policy and Storage Policy copy.

For more information, see Export Media From a List.

EXPORT MEDIA USING VAULTTRACKER AND VAULTTRACKER ENTERPRISE

The **VaultTracker** license provides the capability to track media movement between two locations. It is also used to export media.

The **VaultTracker Enterprise** license provides the capability to track media movement between several locations. In addition to the standard VaultTracker features, it also provides several advanced capabilities.

You can export media using the VaultTracker Feature software and VaultTracker Enterprise Feature in the following ways:

- using the **Export Media Wizard**
- using the **Export Media from a List** feature
- using **VaultTracker Policies**
- after Data Protection and Auxiliary Copy Operations (VaultTracker Enterprise Feature only)

All three methods provide the necessary options to run the export operation immediately or schedule the export operation to run for a later time.

You can configure the number of times an export operation must retry before it is aborted, and the retry interval minutes using the **Export Operation Retry Count** and the **VaultTracker feature export retry interval in minutes** options from the Media Management Configuration (Service Configuration) dialog box available in the **Control Panel**.

When media is exported, the option to use auto-acknowledge pending media movement action is provided. Additionally, VaultTracker Enterprise provides the capability of using virtual mail slots.

For step-by-step instructions on exporting media using VaultTracker and VaultTracker Enterprise, see the following:

- Create a Tracking Policy
- Export Media using the Export Media Wizard
- Export Media From a List using VaultTracker
- Export Media After a Data Protection Operation
- Export Media After an Auxiliary Copy Operation

For in-depth overviews of VaultTracker and VaultTracker Enterprise, see the following:

- VaultTracker
- VaultTracker Enterprise

PREVENT A MEDIA FROM BEING EXPORTED

If for some reason, you would like to prevent media from being exported from a library, the **Prevent Export** option has been provided. If necessary, media that has been prevented for export can also be allowed to be exported using the **Allow Export** option. In the CommCell Browser, the **Prevent Export** and **Allow Export** operations can be performed on a specific media, from the **scratch pool** and the **Media in Library** levels.

SCHEDULING MEDIA EXPORT

Scheduled media export can be performed using VaultTracker.

Appropriate event messages to indicate the start and completed/failed status of a scheduled media export job are logged in the **Event Viewer**.

Do not use the Schedule Media Export operation on a library which does not have a mail slot.

For more information on creating schedules, see Scheduling.

MARK MEDIA EXPORTED

Use this feature to mark all the media in a library or in all the libraries as exported. This feature is useful when you wish to replace a MediaAgent or a library. In such situations, you can mark all the media in a library as exported, before changing the data paths for all the storage policy copies that access the MediaAgent or library. (See Change Data Path for information.)

As this option logically marks all the media as exported in the CommServe database it will enable you to re-import the media into the library after changing the data paths.

SET MEDIA LOCATION

Use this feature to perform the following:

- To pre-define the location, export location or container for media available in a library. This will ensure that the export locations are pre-set for the media.
- To re-define a previously defined location or container.
- To define the export location for exported media.

This operation can be performed in the CommCell Browser from the Library level, or at the Exported Media group level or individually for the specific media.

See Set Media Location in Bulk and Set Media Location for a Specific Media for step-by-step instructions.

EXPORTED MEDIA POOL

The Exported Media pool is the logical repository for all media which were previously discovered and subsequently exported from the library.

From the CommCell Console, you can view the properties such as the media location, container, barcode, Storage Policy/Storage Policy Copy, last write time, and size of stored data for the media listed in this pool.

In addition the following operations can be performed on the media available in the **Exported Media** pool:

- View the contents
- Move the media
- Move Media to Library
- Delete the media
- Mark the media bad
- View the media properties
- Mark media full
- Mark Media Appendable
- Update Media Barcodes
- Set Scratch (for libraries attached to the ACSLS Server)

For Stand-alone drives, all the media residing outside the drive will be listed in the Exported Media Pool.

MEDIA WITH DATA MARKED FOR EXTENDED RETENTION

Media containing data that are marked extended retention is displayed with the suffix (E). This will help you identify media containing data marked for extended retention. See Tape Handling for more information.

CREATING AN EXPORTABLE MEDIA SET

It may be necessary to export a set of media, either a one-time operation or scheduled export operation. For example, to export the daily backups to an offsite storage location. This can be accomplished using Export Media Using VaultTracker.

In addition you can use the following options, if the daily backups should be directed to a new set of media, which is in turn exported using a scheduled export operation.

- Enable the **Start New Media** option, which is available from the **Media** tab of the **Advanced Backup Options** dialog box. This dialog box can be accessed when the job is scheduled using either a regular Schedule or a Schedule Policy, or when a data protection job is run immediately.

  Consider the following when the you select the **Start New Media** option:

  - For an individual job the job will use a new media.
  - For a scheduled job at the backup set level, all jobs that belong to the schedule from that backup set will go to a new media.

  - For a schedule policy, all jobs that run from that schedule policy, for the specific run of that schedule policy, will go to a new media. See
- In addition you can use also enable the **Mark media full after successful operation** option and the **Allow other schedule to use media set** options, if necessary. These options are useful when several data protection jobs are started at the same time by a schedule or schedule policy and the associated data must be written to the same media set.
  - When the **Mark media full after successful operation** option is enabled, the system marks the media as full 2 minutes after the completion of a job. If another data protection job is queued or started within the 2 minute period, the media will be used by that job.
  - When the **Allow other schedule to use media set** option is also enabled, (this option can be enabled only if the **Mark media full after successful operation** option is enabled) jobs from other schedules can also use the same media set.

  Consider the following example:

  - Schedule Policy 1, with the **Mark media full after successful operation** option enabled initiates 2 data protection jobs - job 1 and job 2
  - Schedule Policy 2, with the **Mark media full after successful operation** option *not* enabled initiates 2 data protection jobs - job 3 and job 4

  If the **Allow other schedule to use media set** option is also *not* enabled, jobs 1 and 2 will be written to a new media and jobs 3 and 4 may or may not be written to the same media, depending on whether the job gets a reservation for the operation within the 2 minute interval.

OTHER CONSIDERATIONS

By default, the MediaAgent retains the container and export location associated with the Media. These associations are viewable from the Media Properties - General tab. If necessary, you can enable a global option in the library from the Library Properties -Media tab, to automatically remove these associations when the media is brought back in to the library.

AUDIT TRAIL

Operations performed with this feature are recorded in the Audit Trail. See Audit Trail for more information.

Export Media - How To

Topics | How To | How Do I | Related Topics

Export Media Wizard

Export Media using the Export Media Wizard

Export Select Media

Export a Specific Media

Export Media From a List

Export Media using VaultTracker

Create a Tracking Policy

Export Media From a List using VaultTracker

Export Media After a Data Protection Operation

Export Media After an Auxiliary Copy Operation

Export Media Operations

Set Media Location in Bulk

Set Media Location for a Specific Media

Schedule an Export Media Operation

Prevent a Media From Being Exported

Mark Media as Exported

Move Media to Library

EXPORT MEDIA USING THE EXPORT MEDIA WIZARD

Required Capability: Library Management

➡ To export media from a library using the Export Media Wizard:

1. From the CommCell Browser, right-click the library from which you want to export media, and then click **Export Media**.

   OR

   The **Export Media Wizard** is displayed.
2. From the **Export Media** window in the **Export Media Wizard**, choose whether or not to use VaultTracker to export media.
   - If you choose to export media using VaultTracker, the **Export Media Wizard** guides you through the process of creating tracking policies, choosing media movement criteria, selecting destination and tracking options, etc.
   - If you choose not to export media using VaultTracker, the **Export Media Wizard** guides you through the process of exporting specific media using the **Export Media List**.

     You can also access the **Export Media Wizard** by right-clicking the media you wish to export in the **Media in Library** node and selecting **Export Media**. The **Export Media Wizard** is then displayed.

EXPORT A SPECIFIC MEDIA

Required Capability: Library Management

➡ To export a specific media:

1. From the CommCell Console select the media you wish to export from one of the following pools or dialog boxes:
   - **Media in Library** (discovered and undiscovered media) pool
   - **Scratch pools**
   - **Cleaning Media** pool
   - **Retired Media** pool
   - **Assigned Media** pool
   - **Media List** dialog box which appears when you select the **View Media** option that appears when you right-click a Storage Policy copy.
   - **Media List** dialog box which appears when you select the **Change Data Path** option that appears when you right-click a Storage Policy copy.
   - **Media Used By Job ID** dialog box which appears when you select the **View Media** option from the **Data Protections Job History**, **Backup Job History,** or **Data Migration History** windows.
2. Right-click the media that you want to export, and then click **Export.**
3. In the **Export Media** dialog box, enter an optional description of the location outside the library where the media will be stored.
4. Click **OK.**

   The location field is for display purposes only, to help you keep track of exported media. The MediaAgent has no control over media once they leave the library; it is your responsibility to ensure that exported media are stored in the location entered.
5. An **Export Media** prompt appears, prompting you remove the media. Do one of the following:
   - If you are exporting through a mail slot, click **OK**, wait for the media to be moved to the mail slot, and then remove them from the library.
   - If you are removing media directly, click **OK**, open the library door, remove the media that you want to export, and then close the door.

EXPORT MEDIA FROM A LIST

Media can be selected from a list of media and exported. This is useful when you wish to export several media at the same time and know either the media's barcode, or slot number in which the media resides. This task can be performed from the following levels in the CommCell Console:

Required Capability: See Capabilities and Permitted Actions

➡ To export media from a list:

1. From the CommCell Browser, right-click one of the following from which you want to export media, and then click **Export Media**.
   - **Media List** dialog box which appears when you select the **View Media** option that appears when you right-click a Storage Policy copy.
2. From the Export Media List dialog box, select one or more media that you want to export from the **Select Media to be Exported** list.
3. If the library is a blind library, select the **Verify Media** option. When you select this option, the On Media Label (OML) in the media is checked to ensure that the Unique ID matches the Unique ID of the selected media. The media is exported only if the verification is successful.

4. You can enter an optional comment about the location to which you are moving the media (e.g., Shelf 26 in Storage Room) in the **Outside storage location** field.

   The location field is for display purposes only, to help you keep track of exported media.

5. Click **OK**.
6. An **Export Media** prompt appears, prompting you remove the media. Do one of the following:
   - If you are exporting through a mail slot, click **OK**, wait for the media to be moved to the mail slot, and then remove them from the library. If you are exporting multiple media, they will be delivered to the mail slot one by one until all have been exported.
   - If you are removing media directly, click **OK**, open the library door, remove the media that you want to export, and then close the door.

     In the case of a bulk export (multiple media), some libraries require that you open the mail slot and remove each media individually, as it is delivered. This is true even if the mail slot can hold multiple media. If your library has this requirement and you fail to remove a media within the export media timeout period, the operation times out (i.e., the operation is terminated and a message is sent to the Event Log reporting the failure).

EXPORT MEDIA FROM A LIST USING VAULTTRACKER

Required Capability: See Capabilities and Permitted Actions

To export media from a list using VaultTracker:

1. Initiate an Export Media operation as described in Exporting Media From a List.

   An export media operation can be run immediately or scheduled using the scheduling options.

2. From the **Export Media List** dialog box, click **Advanced**.
3. From the Advanced Options dialog box, click the **Use VaultTracker for export** option.
4. Click the **Use Virtual Mail Slots** option to automatically move the media to a virtual mail slot in the library. Virtual mail slots are defined in the Library Properties (Media) tab.
5. Click the **Auto-acknowledge** option if you want the system to automatically acknowledge all Pending movement actions.
6. Select a **Container** if the media is added to a Container.
7. Click the **Track Transit** option and select the transit location from the list, to track the transit information. Transit locations can be entered using the Export Location Details dialog box.
8. Click **OK** to save the information.

- If the auto-acknowledge option is enabled, the system will automatically acknowledge all pending actions associated with the media movement if both source and destination is a location. If the source is a library, the pending actions will be automatically acknowledged when the media is removed from the library.
- If the auto-acknowledge option is not enabled, the Pending Actions are displayed on the right pane of the CommCell Browser, when you click the **Action** icon under **VaultTracker**.

You must record the status of the media as it goes through the various stages, as described in Monitor and Record the Status of a Media.

EXPORT MEDIA AFTER A DATA PROTECTION OPERATION

Required Capability: See Capabilities and Permitted Actions

To export media after a data protection operation:

1. From the CommCell Browser, right-click the subclient for which you wish to perform a data protection operation, and then click **Backup/Migrate** from the shortcut menu.

   Data Protection operations can be initiated immediately or scheduled using the scheduling options.

2. From the **Backup Options/Migrate Options** dialog box, select the necessary options.
3. Click **Advanced**.
4. From the **Advanced Backup Options/Advanced Migration Options** dialog box, click the **Export Media after the job finishes** option.

5. If necessary, select the option to **Exclude Media Not Copied**.
6. If necessary, select the necessary **Media Status**.
7. Select the **Export Location** from the list. Export locations can be entered using the Export Location Details dialog box.
8. Click the **Track Transit** option and select the transit location from the list, to track the transit information. Transit locations can be entered using the Export Location Details dialog box.
9. Click the **Use Virtual Mail Slots** option to automatically move the media after the data protection operation, to a virtual mail slot in the library. Virtual mail slots are defined in the Library Properties (Media) tab.
10. If you wish to filter media based on its retention, select the appropriate option.
11. Click **OK** to save the information.

Once the data protection operation completes, the Pending Actions (for tracking the associated media) are displayed on the right pane of the CommCell Browser, when you click the **Action** icon under **VaultTracker**.

You must record the movement action as described in Monitor and Record the Status of a Media.

EXPORT MEDIA AFTER AN AUXILIARY COPY OPERATION

Required Capability: See Capabilities and Permitted Actions

To export media after an auxiliary copy operation:

1. From the CommCell Browser, right-click the storage policy for which you want to perform an auxiliary copy and then click **Auxiliary Copy**.

   Auxiliary Copy operations can be initiated immediately or scheduled using either the scheduling options or a Schedule Policy.

2. From the **Auxiliary Copy** dialog box, select the necessary options.
3. Click **Vault Tracking**.
4. From the Select Vault Tracking Options dialog box, click the **Export Media after the job finishes** option.
5. If necessary, select the option to **Exclude Media Not Copied**.
6. If necessary, select the necessary **Media Status**.
7. Select the **Export Location** from the list. Export locations can be entered using the Export Location Details dialog box.
8. Click the **Track Transit** option and select the transit location from the list, to track the transit information. Transit locations can be entered using the Export Location Details dialog box.
9. Click the **Use Virtual Mail Slots** option to automatically move the media after the Auxiliary Copy operation, to a virtual mail slot in the library. Virtual mail slots are defined in the Library Properties (Media) tab.
10. If you wish to filter media based on its retention, select the appropriate option.
11. Click **OK** to save the information.

Once the Auxiliary Copy operation completes, the Pending Actions (for tracking the associated media) are displayed on the right pane of the CommCell Browser, when you click the **Action** icon under **VaultTracker**.

You must record the movement action as described in Monitor and Record the Status of a Media.

CREATE A TRACKING POLICY

Required Capability: See Capabilities and Permitted Actions

To create a Tracking Policy:

1. From the CommCell Browser, right-click the **VaultTracker Policies** icon under the Policies node, and then click **New Tracking Policy**.
2. The **VaultTracker Policy** wizard guides you through the process of creating a new Tracking Policy.

- A regular Tracking policy can be created to export media based on the selected criteria.
- A due back Tracking policy can be created to track the movement of spare media, residing outside the library.
- Once created the Tracking Policy must be run or scheduled, as described in Run a Tracking Policy and Schedule a

Tracking Policy.

SET MEDIA LOCATION IN BULK

Required Capability: See Capabilities and Permitted Actions

1. From the CommCell Console right-click the **Exported Media** Pool, and then click **Set Location**.
2. From the Set Export Location dialog box, click the media that you wish to set the export location (or move to a container) from the **Select Media for which you want to set the location** list. (To select multiple media, press and hold down CTRL or SHIFT keys while clicking.)
3. Enable the **New Export Location** or the **Container** option and enter or select the location or container from the list.
4. Click **OK** to save the information.

The export location for the selected media is added/changed. (Export location for a media can be viewed in the General tab of the **Media Properties** dialog box.)

SET MEDIA LOCATION FOR A SPECIFIC MEDIA

Required Capability: See Capabilities and Permitted Actions

1. From the CommCell Console right-click the **Media** for which you wish to set the export location (or move to a container) and then click **Properties**.
2. In the General tab of the **Media Properties** dialog box enter or select the location (or container) from the **Previously Exported to** or the **Container** list.
3. Click **OK** to save the information.

The export location for the media is added/changed.

SCHEDULE AN EXPORT MEDIA OPERATION

Required Capability: See Capabilities and Permitted Actions

To schedule an export media operation:

1. From the CommCell Browser, right-click the library from which you want to export media, and then click **Export Media**.
2. From the Export Media List dialog box, select one or more media that you want to export from the **Select Media to be Exported** list.
3. If the library is a blind library, select the **Verify Media** option. When you select this option, the MediaAgent checks the On Media Label (OML) in the media to ensure that the Unique ID matches the Unique ID of the selected media and exports the media only if the verification is successful.
4. You can enter an optional comment about the location to which you are moving the media (e.g., Shelf 26 in Storage Room) in the **Location** field. Click **OK**.

   > The location field is for display purposes only, to help you keep track of exported media. The system has no control over media once they leave the library; it is your responsibility to ensure that exported media are stored in the location entered.

5. Click the **Advanced** button.
6. From the Advanced Options dialog box, select **Use VaultTracker for export**. Select any other additional options as required.
7. Click **OK**.
8. Click the **Schedule** button.
9. From the Schedule Details tab of the Schedule Details dialog box, select the scheduling options that you want to apply.
10. If you want to review the options that you selected for the job, click the Job Summary tab.
11. To submit the job for scheduling, click **OK**.

PREVENT A MEDIA FROM BEING EXPORTED

Required Capability: See Capabilities and Permitted Actions

1. From the CommCell Browser locate the media you wish to prevent from being exported from the **Media By Groups** pools or the **Media in Library** group.
2. Right-click the media and then click **Prevent Export**. Click **Yes** in the **Confirm** promt.

3. In the **Prevent Export** dialog box:
   - Select the option **Infinite** to prevent the media from being exported for an infinite period of time.
   - To provide an expiration date, select the desired date and time until which the media would be prevented from export. Also, select the time zone corresponding to the expiration date.
4. Click **OK.**

   The media will be prevented from being exported and are displayed with a green highlight in the CommCell Browser.

   If necessary you can remove the prevent export status by right-clicking such media and then clicking the **Allow Export** option.

MARK MEDIA AS EXPORTED

Required Capability: See Capabilities and Permitted Actions

➨ To mark media as exported

1. You can mark media as exported for the following:
   - All the libraries in the CommCell:

     From the CommCell tree, right- click the **Libraries** node and then click **Mark Media Exported**.
   - A specific library in the CommCell:

     From the CommCell Console, right- click the library for which you wish to mark the media as exported and then click **Mark Media Exported**.
2. Click **Yes** in the **Confirm** prompt warning you that the operation will mark all the media as exported.
3. In the **Export Media** dialog box, enter an optional description of the location outside the library where the media will be stored.
4. Click **OK.**

   All the media in the library is marked as exported.

MOVE MEDIA TO LIBRARY

To move the Exported media to a library:

1. From the right pane of the CommCell Console, right click the media that you want to move and click **Move to Library**.

   You can select multiple media simultaneously. Hold **Ctrl** key and select multiple media from the right pane of the CommCell Console. Then right click the selected media and click **Move to Library**.
2. From the **Move Media to Library** dialog box, select the library to which you want to move the media. This dialog box displays list of libraries which are compatible to the selected media.
3. Click **OK**. The media is moved to the selected library.

Full Scan

Topics | How To | Related Topics

Full Scan operation identifies the slot location and barcode or media identifier of every media detected within the library. This information is used to prepare the new media list (from which media can be discovered for the CommCell) and information on the location of known media.

> The full scan only finds the media that are contained within a library. However, in order to use new media, additional information is collected by the discovery operation. See Discover Media for comprehensive information on media discovery.

The full scan operation, can be in a full or update mode, and may take a few minutes depending on the settings in the individual library. Usually a full scan operation takes place when either of the following occurs:

- You open and close the library door. (full or update)
- You turn on the library’s power. (full)
- You request a reset library operation (full or update), although not all libraries invoke the full scan command on a reset library command.
- You request an import or export media operation. (update)
- When you specify the Full Scan operation from the CommCell Console. (full)

In addition many library models conduct a full scan operation when any of the following occurs:

- You first install and configure the library.
- The CommServe’s Library and Media Manager service or MediaAgent Services are restarted.

When a full scan is in progress, the library status is displayed as `offline` until the procedure completes successfully. This means that new data protection operations or data recovery operations that access the library cannot start until the full scan operation completes. Usually, the full scan operation does not affect media that are already mounted in drives. A data protection operation or data recovery operation that is in progress when the full scan is initiated can continue as long as it does not need to access unmounted media. However some library models may force the drive to unload resulting in the data protection operation or data recovery operation using the drive to fail. Appropriate Event Messages to indicate the library’s offline/online status during a full scan operation is logged in the Event Viewer.

Full Scan - How To

Topics | How To | Related Topics

PERFORM A FULL SCAN OPERATION

To perform a full scan:

1. From the CommCell Browser, right-click the library for which you wish to perform the full scan and then click **Full Scan**.

   You can track the progress of the job from the Event Messages logged in the Event Viewer.

Import Media

Topics | How To | Related Topics

OVERVIEW

> Ensure that the barcode used in the media is compatible with the library's barcode reader; see the library manufacturers documentation for a list of compatible label formats.

Importing is the process by which you move media that are outside a library into storage slots within the library. There are two ways of importing media:

- You can import media through the library's mail slot (if available)
- You can open the library door and manually insert media into storage slots in the library

IMPORT MEDIA THROUGH THE LIBRARY MAIL SLOT

Importing media through a mail slot offers an advantage - the inventory update that is triggered by a mail slot import is much less time-consuming than the full inventory operation that is triggered when you open and then close the library door.

You can use one of the following methods to import media using the library mail slot:

- To manually import media , use the **Import** command from the CommCell Browser. (See Import Media for step-by-step instructions.)
- To automatically move the media from the mail slot to a storage slot in the library, disable the **Prevent Auto Import of Media from mail slot** option. (See Library Properties (Advanced) tab for more information.)

  Once the media is available in the storage slot, the MediaAgent software must discover the media in order to use the media in the library. This is done automatically if the **Enable Auto-Discover** option for the library is enabled. (See Enable (or Disable) Automatic Media Discovery for step-by-step instructions.) This will automatically move the media to the default scratch pool or an appropriate scratch pool based on the bar code patterns, if bar code patterns are defined. (See Managing Media in a Library for details.)

  If the **Enable Auto-Discover** option for the library is not enabled, the media will be displayed (with a '?' icon) in the **Media in Library** pool in the CommCell Browser. You must subsequently discover the media, in order to use the media in the library. (See Discover Media from the CommCell Console and Discover a Specific Media Within a Library for step-by-step instructions.

  See Also: Discover Media

DIRECTLY INSERT MEDIA BY OPENING THE LIBRARY DOOR

Under certain circumstances you may want to open the library door even though a mail slot is available. For example, if you want to add many media to a library at once, it may be faster to open the door than to use the mail slot.

Once again, the media will be automatically discovered, if the **Enable Auto-Discover** option for the library is enabled. (See Enable (or Disable) Automatic Media Discovery for step-by-step instructions.)

If this option is disabled, the media will be displayed (with a '?' icon) in the **Media in Library** pool in the CommCell Browser. You must subsequently discover the media, in order to use the media in the library. (See Discover Media from the CommCell Console and Discover a Specific Media Within a Library for step-by-step instructions.

> If you are not using a mail slot, be careful not to open the library door while media are mounted in drives within the library. In some library models opening the door causes the library to unmount all media, even those that are in active use. This can cause database inconsistency and failure of the running job(s).
>
> Inserting media in and closing the mail slots of some libraries may trigger a full inventory operation (rather than an inventory update).

OTHER CONSIDERATIONS

When a media is imported, the system assigns it in one of the following ways:

- If it is a media associated with the CommCell, which was previously exported, it will be assigned to the scratch pool or a storage policy copy to which it was assigned before it was exported.
- If the media is a new media the system assigns it to the scratch pool that you select (manual discovery) or to the default scratch pool (automatic discovery). (For additional information, see Discover Media.)
- When a previously discovered spare media is moved between libraries, if the media matches the media type of the default scratch pool in the new library, then it is assigned to the default scratch pool. Otherwise, it is assigned to any user-defined scratch pool of matching media type. If there is no scratch pool of matching media type, then the media is assigned to the default scratch pool.
- By default, the MediaAgent retains the container and export location associated with the Media. These associations are viewable from the Media Properties - General tab. If necessary, you can enable a global option in the library from the Library Properties -Media tab, to automatically remove these associations when the media is brought back in to the library.

IMPORT CLEANING MEDIA

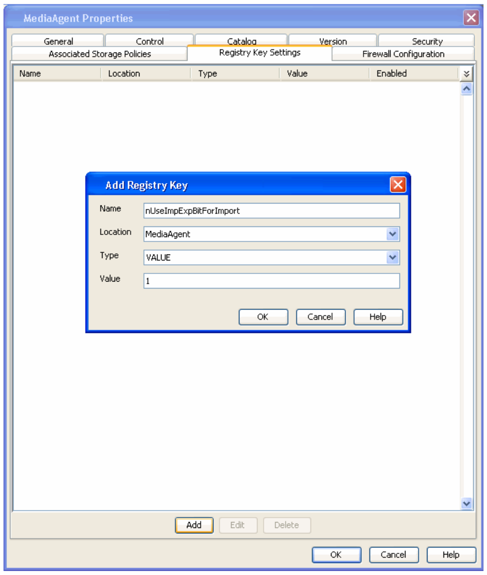
When you import a cleaning media, the system automatically assigns it to the cleaning media pool. For comprehensive information on cleaning media, see Cleaning Media.

IMPORT NEW MEDIA AFTER RESETTING A LIBRARY WITH I/E PORT

In libraries with I/E port, the media is not imported back to the library after a reset operation to prevent exported media from being re-imported to the library. However, if you have new media in I/E port, you may want to import only the new media. Follow the steps below to enable the import operation.

1. From the CommCell Browser, navigate to **Storage Resources | MediaAgents**.
2. Right-click the <***MediaAgent***> computer, and then click **Properties**.
3. Click the **Registry Key Settings** tab.
4. Click **Add**.
5. In the **Name** field, type `nUseImpExpBitForImport`.
6. In the **Location** list, select **MediaAgent**.
7. In the **Type** list, select **Value.**
8. In the **Value** field, type `1`.
9. Click **OK**.

If the library is shared between multiple MediaAgents, then repeat the above steps in all the MediaAgent computers that share the library.



Add Registry Key

Name: nUseImpExpBitForImport

Location: MediaAgent

Type: VALUE

Value: 1

Back to Top

Import Media - How To

Topics | How To | Related Topics

Import Media

Enable Automatic Media Discovery During Library Configuration

Enable (or Disable) Automatic Media Discovery

Discover Media from the CommCell Console

Discover a Specific Media Within a Library

IMPORT MEDIA

Required Capability: See Capabilities and Permitted Actions

> If you are not using a mail slot, be careful not to open the library door while media are mounted in drives within the library. In some library models (e.g., ATL 200, ATL 500) opening the door causes the library to unmount all media, even those that are in active use. This can cause database inconsistency and failure of the running job(s).
>
> Inserting media in and closing the mail slots of some libraries may trigger a full inventory operation (rather than an inventory update).

To import media into a Tape or Optical library:

1. From the CommCell Browser, right-click the library (or the scratch pool of the library) into which you want to import media, and then click **Import Media** from the short-cut menu.

   > All the newly imported media will be automatically moved to the default scratch pool, if the **Enable Auto-Discover Media into default scratch pool** option is enabled in the Media tab of **Library Properties** dialog box, . Use the **Move Media** option to move the media to another scratch pool. If you have cleaning media make sure that you move it to the **Cleaning Media** pool.

2. An Import Media prompt appears, advising you to do one of the following:
   - If you are importing through a mail slot, insert one or more media into the mail slot and wait for them to be moved to storage slots. Do not click OK until all of the imported media have been moved to storage slots.

     > If you click **OK** in the Insert Media prompt before the media are moved to storage slots, the MediaAgent will not discover the media. For information on discovering media, see Discover Media from the CommCell Console.

     After all media are transferred to storage slots, click **OK** in the Import Media prompt.
   - If you are inserting media directly, open the library door, insert media into storage slots, and then close the door. Click **OK** in the Import Media prompt.
3. A warning message is displayed to move cleaning media to cleaning media pool. Click **OK**.
4. If the imported media were previously discovered, their barcodes are displayed in the library inventory in the right pane of the CommCell Browser. Otherwise, the media must be discovered.
   - If you imported undiscovered media through the mail slot (and you did not click OK in the Insert Media prompt until the media were moved to storage slots), the MediaAgent automatically discovers the media. In the Select Media Type dialog box that appears, select the hardware type of the new media from the **Media Type to be Imported** list and the scratch pool to which you want the media assigned from the **Destination Scratch Pool** list. The total number of undiscovered media available in the library is displayed in the **No. of media in Free Media Pool** field. Specify the number of media you would like to discover in the **No. of media to be discovered** field. Click **OK**.
   - If you opened the library door and inserted media directly, or if you imported through a mail slot and clicked OK before the media were moved to storage slots, you must manually discover media as described in Discover Media from the CommCell Console.

ENABLE AUTOMATIC MEDIA DISCOVERY DURING LIBRARY CONFIGURATION

Required Capability: Capabilities and Permitted Actions

To discover media within a library:

1. Display the Library and Drive Configuration window.
2. Detect the devices. Use Detection or Exhaustive Detection as required.
3. Configure the library as described in Configure Devices.

   During the configuration process, if the library has a barcode reader, the **Discover Media Options** dialog box is displayed.

   Perform one of the following:
   - To automatically discover the media in the library, select the default media type and then click **Yes**.
   - To manually discover the media, click **No**. See Discover Media from the CommCell Console for step-by-step instructions on manually discovering media in a library.

     Ensure that media is discovered, before using the library for a data protection operations.

   If the library does not have a barcode reader, another **Discover Media Options** dialog box is displayed.

   Select the correct media type available in the library and then click **OK**.

Enable or Disable Automatic Media Discovery

Required Capability: See Capabilities and Permitted Actions

➤ To enable automatic media discovery:

1. From the CommCell Browser, right-click the library for which you wish to enable automatic media discovery, and then click **Properties**.
2. Click the Media Usage tab.
3. From the **Auto-Discovery of Media** region, click **Enable Auto-Discovery of Media into default scratch pool** option. (Clear this check box to disable this option.)
4. Select the default media type available in the library from the **Default Media Type** list.

   Note that the media available in a library must be compatible with the drives attached to the library.
5. Click **OK** to save the changes.

   When you subsequently import media, the imported media is automatically moved to the default scratch pool.

Discover Media from the CommCell Console

You can use the following procedure to:

- Discover all media within a library
- Discover a partial set of media within a library

Required Capability: Capabilities and Permitted Actions

➤ To discover media within a library:

1. From the CommCell Browser, right-click the library whose media you want to discover, and then click **Discover Media**.
2. If one or more new media are discovered, the system displays the Discover New Media dialog box and prompts you for media information.
3. Select the hardware type of the new media from the **New Media Type** list and the scratch pool to which you want the media assigned from the **Destination Scratch Pool** list.
4. The total number of undiscovered media available in the library is displayed in the **No. of media in Free Media Pool** field. Specify the number of media you would like to discover in the **No. of media to be discovered** field.
5. Click **OK**.

You can also discover the media from the **Library and Drive Configuration** window. See Discover Media from the Library and Drive Configuration Window for more information.

Discover a Specific Media Within a Library

Required Capability: Capabilities and Permitted Actions

➤ To discover a specific media within a library:

1. From the CommCell Browser, locate the library whose media you want to discover in the **Libraries** level.
2. Navigate to the **Media in Library** pool.

   All the media available in the library is displayed in the right-pane of the CommCell Console.

   Right-click the (undiscovered) media and then click **Discover**.
3. From the Discover New Media dialog box, select the Media Type and Scratch Pool to which the media must be moved.
4. Click **OK**.

The media is discovered and assigned to the specified scratch pool.

Mark Library Fixed

Topics | How To | Related Topics

When the number of software or hardware errors exceed the preset threshold values established for the library, the status of the library is automatically changed as **Offline** with the appropriate **Offline Reason**. In such a situation, it is essential to identify and correct the related hardware or software problem. Once the hardware or software problem is addressed, you must notify the MediaAgent using the **Mark Library Fixed** option, to reset the counters that keep track of library events and bring the library online.

See Library Maintenance Threshold Parameters for information on setting up the threshold values for the library.

Mark Library Fixed - How To

Topics | How To | Related Topics

Mark a Library as Fixed

Required Capability: See Capabilities and Permitted Actions

To mark a library as fixed:

1. From the CommCell Browser, right-click the library that you have fixed, and then click **Mark Library Fixed**.
2. Click **Yes** in the Confirm prompt that appears. This will reset the counters for the library.

Reset Library

Topics | How To |

OVERVIEW

You can use the Reset command when you wish to unmount all the media mounted in the drives, and reset all the drives so that they are ready for use. The reset library option is especially useful when you have stuck tapes in the drives. Note however, that the reset library operation is library dependant and hence not the same for all the library models.

Reset library causes the system to perform the following operations:

- The library status is marked as **offline**
- Within the library, all the media mounted in its drives are unmounted
- In some situations an inventory process may be triggered, and once the inventory process is completed, the library status is marked back as **online**.

Reset library operation will fail if there are jobs running on this library.

Reset Library - How To

Topics | How To |

RESET A LIBRARY FROM THE COMMCELL CONSOLE

Required Capability: Library Management

To reset a library:

1. Be certain that the library that you want to reset is not in use. Use the Job Controller to find and stop/kill any jobs that use the library. For more information, see Job Controller.
2. From the CommCell Browser, right-click the library that you want to reset, and then click **Reset Library**.
3. A Confirm Reset prompt appears, informing you that this procedure will unmount any media that are mounted, an operation which may take some time. If you are sure that you want to reset the library, click **Yes**.

   If any drive within the library is active, an error message will be displayed.

Scratch Pools

Topics | How To | Related Topics

Default Scratch Pools

A scratch pool is a repository of media that are available for use. When a data protection, synthetic full, or auxiliary copy operation requires new media, the system takes one from a scratch pool. Media may be:

- Assigned to a scratch pool when they were imported and discovered in the CommCell.
- Logically reassigned from one scratch pool to another scratch pool.
- Returned to a scratch pool by the system when all of its data are pruned or deleted. (For additional information, see Media Recycling.)

Every library has a default scratch pool, which is automatically created when the library is configured. When the system creates a storage policy for the library (e.g., when the library or one of its drive pools is configured), the primary storage policy copy is associated with the default scratch pool. In addition, when you import new media into the library, this is the scratch pool to which they are assigned (unless you specify otherwise). You can create any number of additional scratch pools, and assign these to different storage policy copies that access the library. You can also designate a user-defined scratch pool as the default for the library. See Change the Scratch Pool Associated With a Storage Policy Copy for step-by-step instructions.

New Scratch Pools

A scratch pool is a repository of media that are available for use. Every library has a default scratch pool, which is created when the library is configured. You can create any number of additional scratch pools, and assign these to different storage policy copies that access the library. You can also designate a user-defined scratch pool as the default for the library.

The ability to create scratch pools and assign them to specific storage policy copies enables you to ensure that critical operations always have the media that they need. For example, assume that you regularly back up both a file server containing mission-critical data and a number of user PCs. You may want to prevent situations in which data secured from less important user PCS use up all available media, causing vital data protection operations on file server to fail. You can do this by creating a scratch pool specifically for the storage policy copies that conduct data protection operations on file servers. You can, if necessary, delete these non-default scratch pools.

You can move media between scratch pools. In the example above, if you noticed that the supply of media in the scratch pool dedicated to the file server was getting low, you could logically reassign media from another scratch pool to the file server pool.

You can also verify the media to confirm whether the media information displayed in the CommCell Console matches the OML in the media.

Low Watermarks

You can also establish a low watermark for each scratch pool. This parameter represents the minimum number of media that should be available inside the library for the scratch pool at all times. If the number of available media in the scratch pool falls below the low watermark, the system logs a message in the `Event Viewer` and generates the `MediaAgents (Insufficient Storage)` alert, if configured. You can view the status of media available in the scratch pools by generating the `Scratch Pool Report`.

The low watermark for all user created scratch pools in the CommCell can be established in the **Default low-water mark for newly created Scratch Pools** option established in the **Service Configuration** tab of the **Media Management Configuration** dialog box in the **Control Panel**. If necessary, you can modify the low watermark for the individual scratch pools. (See Specify the Minimum Number of Media in a Scratch Pool for step-by-step instructions.)

When you establish a low watermark, consider the media requirements of all operations (e.g., data protection operations, auxiliary copies, synthetic full backups) that draw from the scratch pool. The low watermark should be high enough to ensure that you will be notified of the need for more media while there are still enough media available to allow running operations to complete. For example, if the operations that access a particular scratch pool regularly fill two media every week, you might set the low watermark at three. This way, you will be alerted every week to add more media to the scratch pool while it still contains sufficient media to handle its normal operational load.

Related Reports

SCRATCH POOL REPORT

The Scratch Pool Report provides a list of the contents and low watermarks of scratch/cleaning pools.

Scratch Pools - How To

Topics | How To | Related Topics

CREATE NEW SCRATCH POOLS

Required Capability: See Capabilities and Permitted Actions

To create a scratch pool:

1. From the CommCell Browser, right click the Media By Groups icon for the library in which you want the scratch pool created, and then click **New Scratch Pool** from the short-cut menu.
2. In the Spare Group Properties dialog box, enter the name of the new scratch pool in the **Name** field. Optionally, you can set the low watermark in the **Low Watermark** field.

   When you first create a scratch pool, it is empty. Before the scratch pool can be used as a source of fresh media, you must either import media into it from outside the library or move media into it from another scratch pool.

SPECIFY THE MINIMUM NUMBER OF MEDIA IN A SCRATCH POOL

Required Capability: See Capabilities and Permitted Actions

To specify the minimum number of media in a scratch pool:

1. From the CommCell Browser, right-click the scratch pool for which you wish to specify the minimum number, and then click **Properties**.
2. From the General tab use the option provided in **Watermark for Spare Media in the pool** area to establish a minimum number of media in the scratch pool.
3. When you are satisfied with your changes, click **OK**.

MOVE A MEDIA FROM ONE SCRATCH POOL TO ANOTHER

Required Capability: See Capabilities and Permitted Actions

To move a media from one scratch pool to another:

1. In the left pane of the CommCell Browser, select the scratch pool containing the media that you want to move. The contents of the scratch pool are displayed in the right pane of the Browser.
2. From the right pane of the CommCell Browser, right-click the media that you want to move, and then click **Move**.
3. In the Move Media dialog box, select the scratch pool to which you want to move the media. If it is cleaning media, select Cleaning Media pool.
4. Click **OK** to complete the transfer.

   The selected media is reassigned to the destination scratch pool.

MOVE MEDIA IN BULK FROM ONE SCRATCH POOL TO ANOTHER

Required Capability: See Capabilities and Permitted Actions

To move a number of unspecified media from one scratch pool to another:

1. From the CommCell Browser, right-click the scratch pool from which you want to move media (i.e., the source pool), and then click **Move Media** from the short-cut menu.
2. In the Move Media dialog box, enter the number of media to be moved in the **No. of Media to be moved** field. Select the scratch pool into which you want to move the media from the **Destination Scratch Pool** list.
3. Click **OK** to complete the transfer.

   The selected media is reassigned to the destination scratch pool.

DELETE A SCRATCH POOL

Required Capability: See Capabilities and Permitted Actions

The following scratch pools cannot be deleted:

- A scratch pool that is associated with a storage policy copy.
- A scratch pool that has been designated as the default scratch pool for the library.

To delete a scratch pool:

1. From the CommCell Browser, right-click the scratch pool that you want to delete, and then click **Delete**.
2. A confirmation prompt appears, asking if you are sure that you want to delete this scratch pool. Click **Yes** to delete.

   The scratch pool is deleted and the CommCell Browser display is updated and all of its spares are displayed as undiscovered media.

CHANGE THE DEFAULT SCRATCH POOL

Required Capability: See Capabilities and Permitted Actions

To change the default scratch pool:

1. From the CommCell Browser, right-click the library for which you wish to change the default scratch pool, and then click **Properties**.
2. Select the name of the scratch pool that you wish to designate as the default scratch pool from the **Default Scratch Pool** list.
3. Click **OK** to save the changes.

CHANGE THE SCRATCH POOL ASSOCIATED WITH A STORAGE POLICY COPY

Required Capability: See Capabilities and Permitted Actions

To change the scratch pool for a storage policy copy:

1. From the right pane of the CommCell Browser, right-click the storage policy copy for which you wish to change the scratch pool, and click **Properties**.
2. From the General tab of the **Copy Properties** dialog box, select another scratch pool from the **Scratch Pool** list.
3. Click **OK** to save your changes.

Update Media Barcodes

Topics | How To | Related Topics

The ability to update barcodes associated with the media ensures that the data available in the media is accessible. There are several situations in which the barcode may have to be renamed in order to read the data available in the library. For example:

- When a libraries firmware is upgraded, or when a hardware is replaced a different barcode pattern may apply.

  In such cases, the system automatically updates the media barcodes if the **Automatically update barcodes on firmware changes option** is enabled in the **Advanced** tab of the **Library Properties**. (See Automatically update barcodes on firmware changes for more information.)

  If this option is disabled, and the barcodes are changed after a firmware upgrade all existing media, including media with data and spare media will be marked as exported and a new set of media (with new barcodes) will be listed inside the library. In this situation, you must update the barcodes as described in Manually Updating Media Barcodes after a Firmware Upgrade.
- When performing the Change Data Path operation from one library to another. Although the new library may have compatible drives, it may have a different barcode pattern.
- When data is required to be restored from another compatible library with a different barcode pattern. (See Restore From Anywhere and Restore Data Using a Specific MediaAgent, Library or Drive Pool.)
- When the media is used to restore data in a hot-site with another compatible library. (See MediaAgent Recovery - How To for more information.)

The system provides the ability to

- Rename barcodes in bulk, or
- Rename the barcode associated with an individual media

Update Media Barcodes - How To

Topics | How To | Related Topics

Update Barcodes in Bulk

Required Capability: Capabilities and Permitted Actions

➧ To update the barcodes in a library:

1. From the CommCell Browser, right-click library in which you wish to rename barcodes and then click **Update Barcodes**.
2. Click **Yes** in the confirmation prompt to continue.
3. From the Update Barcodes dialog box, select the whether you wish to add or remove a suffix or prefix from the **Please select Operation** list.
4. Enter the text that should be added or removed in Enter text.
5. Click **OK.**

The barcodes in the library are updated.

Update the Barcode Associated with a Specific Media

Required Capability: Capabilities and Permitted Actions

➧ To update the barcode for a specific media:

1. From the CommCell Browser, right-click media for which you wish to update the barcode and then click **Update Barcode**.
2. From the Update Barcode dialog box, specify the new barcode
3. Click **OK.**

The barcode for the selected media is updated.

MANUALLY UPDATING MEDIA BARCODES AFTER A FIRMWARE UPGRADE

Required Capability: Capabilities and Permitted Actions

➧ To manually update the media barcodes after a firmware upgrade:

1. Note down the prefix or suffix that was changed in the media when the firmware was upgraded.
2. Delete all the spare media in the library with the new barcode format.

   See Delete a Media for step-by-step instructions.
3. Update the barcodes in the library to add or remove the prefix or suffix that was changed in the media when the firmware was upgraded.

   See Update Barcodes in Bulk for step-by-step instructions.
4. After successfully updating the barcodes, perform a full scan of the library.

   See Perform a Full Scan Operation for step-by-step instructions.

The barcodes in the library will be updated.

Library Properties

Topics | How To | Related Topics

OVERVIEW

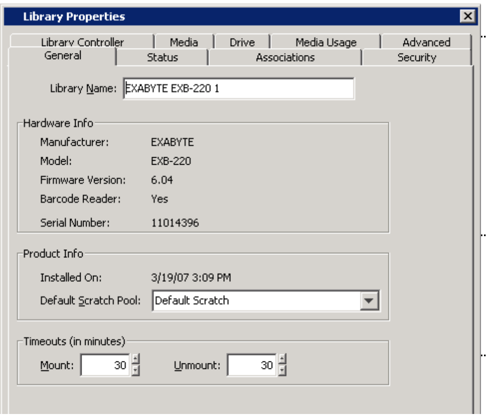
The MediaAgent supports a wide variety of storage units or libraries, which can be grouped into the following general categories:

Library	Typically a multi-drive storage unit that houses multiple media cartridges for extended storage capacity. The physical size of the cabinet, generally determines the number of resident media drives and cartridges. Media movement operation inside the library is performed by a robotic arm, (or media changer) which is controlled by the library controller. Library can be tape or optical library.
Stand-alone drive	Typically a one-drive storage unit with no media storage capability. Media must be manually mounted (inserted) and unmounted (ejected) from the drive. It is also considered as a logical library. Note the following: • Removable Disk Drives are also configured as stand-alone drives. • PnP (Plug and Play) Disks, are also similar to stand-alone drives.
Disk Libraries	A disk library is a virtual library associated with one or more mount paths. The disk library does not represent a specific hardware entity; it is a software entity that contains a list of mount paths through which data can be sent to a disk media. See Disk Libraries for more information.

The following sections describe the properties associated with tape/optical/stand-alone drives. Note that all these options may not apply to all these libraries.

In the CommCell Console and in Books Online, all storage units are referred to as libraries, regardless of type.

GENERAL



Library Name: EXABYTE EXB-220 1

Hardware Info

Manufacturer: EXABYTE

Model: EXB-220

Firmware Version: 6.04

Barcode Reader: Yes

Serial Number: 11014396

Product Info

Installed On: 3/19/07 3:09 PM

Default Scratch Pool: Default Scratch

Timeouts (in minutes)

Mount: 30 Unmount: 30

LIBRARY NAME

The system initially assigns the library name which is derived from the library manufacturer and model. If necessary, you can modify the library name.

If you are using stand-alone drives, we strongly recommend that you physically label each drive using the library name shown in the configuration window. This will help you identify the proper drive when you are prompted to insert a cartridge into a drive.

HARDWARE INFO

The general information about the library, including the library manufacturer, model, firmware version, whether the library includes a barcode reader and the serial number of the library are displayed.

PRODUCT INFO

Product information includes information on the date and time at which the library was configured and the default scratch pool for the library.

Note that the default scratch pool is automatically created when the library and drives are configured. You can create additional scratch pools and designate them as the default scratch pool for the library. For comprehensive information on scratch pools, see Scratch Pools.

TIMEOUTS

A timeout parameter determines how long a job waits for a status response after an operation is requested. If the job does not receive a success or failure status within the timeout period, the job is terminated and a failure message is displayed. You can set the following timeout periods:

- **MOUNTING MEDIA**

  The time period within which media must be moved to a drive and prepared for read/write operations.

- **UNMOUNTING MEDIA**

  The time period within which media must be returned from a drive to a storage slot.

See Modify the Mount and Unmount Timeouts for step-by-step instructions.

DESCRIPTION

You can use the space provided in the description box to record important and reference information about the library.

STATUS

STATUS

The status of the library indicates whether the library is online or offline, and if offline, the reason for the offline status. See View the Library Offline Reason for step-by-step instructions.

You can use the enable/disable indicator to logically enable or disable the library. See Enable (or Disable) the Library for step-by-step instructions.

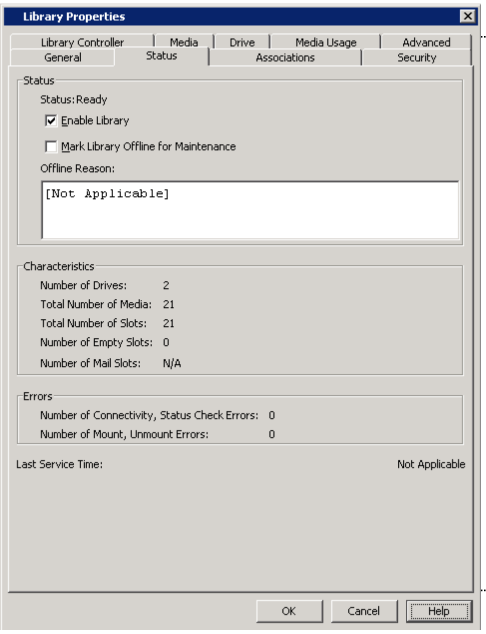
- **MARK LIBRARY OFFLINE FOR MAINTENANCE**

  You can enable this option when you wish to perform routine or other maintenance tasks on devices. This option is available in the MediaAgent, Library and Drive levels and you can appropriately enable them where needed.

  Data protection, data recovery and auxiliary copy operations will not use the associated MediaAgent/Library/Drive, depending on where the option is enabled. However, other administrative tasks on the devices such as Full Scan, Drive Cleaning, Verify Media etc. can be performed, if required.

  When this option is enabled, the system will automatically select an alternate resource (MediaAgent/Library/Drive) if Alternate Data Paths (GridStor) is enabled. If alternate resources are not available, data protection, data recovery and auxiliary copy will remain in the `Waiting` state in the **Job Controller** and will automatically resume when you re-enable the appropriate MediaAgent/Library/Drive.

See Mark MediaAgent/Library/Drive Offline for Maintenance for step-by-step instructions.



Status

Status: Ready

☑ Enable Library

□ Mark Library Offline for Maintenance

Offline Reason:

[Not Applicable]

Characteristics

Number of Drives:	2
Total Number of Media:	21
Total Number of Slots:	21
Number of Empty Slots:	0
Number of Mail Slots:	N/A

Errors

Number of Connectivity, Status Check Errors:	0
Number of Mount, Unmount Errors:	0

Last Service Time: Not Applicable

CHARACTERISTICS

Other library characteristics such as the number of drives, slots, total number of media and empty slots, number of mail slots

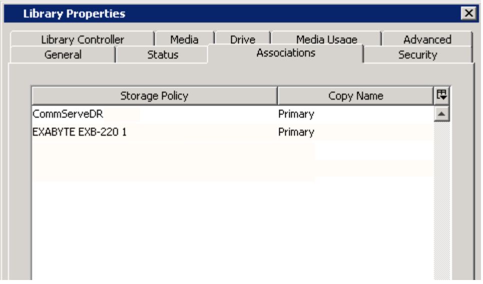
ERRORS

The number of connectivity, status, mount and unmount errors in the library, and the last service time are also displayed.

ASSOCIATIONS

The Association tab provides information about all the storage policy and their copies associated with a library. This information is useful when you deconfigure a library, as all the storage policy copies associated with the library must be deleted, prior to deconfiguring a library.

See View the Storage Policies Accessing a Library for step-by-step instructions.



Storage Policy	Copy Name
CommServeDR	Primary
EXABYTE EXB-220 1	Primary

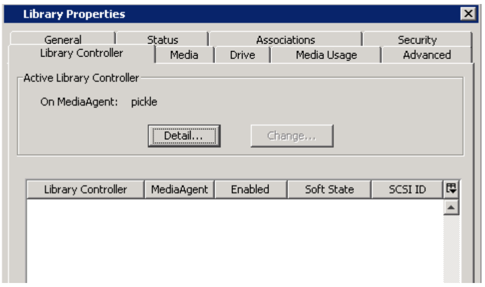
SECURITY

Security allows you to associate a library with one or more CommCell user groups. For a detailed explanation of security, see User Administration and Security.

LIBRARY CONTROLLER

In a SAN environment, the library controller feature can be used to configure the active MediaAgent to automatically switch over to a failover MediaAgent, in the event of a failure in the active MediaAgent. For more information on library controllers, see SAN Attached Libraries.

The MediaAgent checks the library controller based on the value established in the **Library Arm Controller failover interval in Minutes** option from the Media Management Configuration (Service Configuration) dialog box available in the **Control Panel**.



Active Library Controller

On MediaAgent: pickle

Library Controller	MediaAgent	Enabled	Soft State	SCSI ID

MEDIA

MARK MEDIA APPENDABLE

When this option is enabled, a media will be marked as **Appendable** when it is not available in the library and a new media will be used by the job. (If this option is not enabled, the media will be marked as **Full**.) Enabling this option ensures that the media in the library is fully utilized.

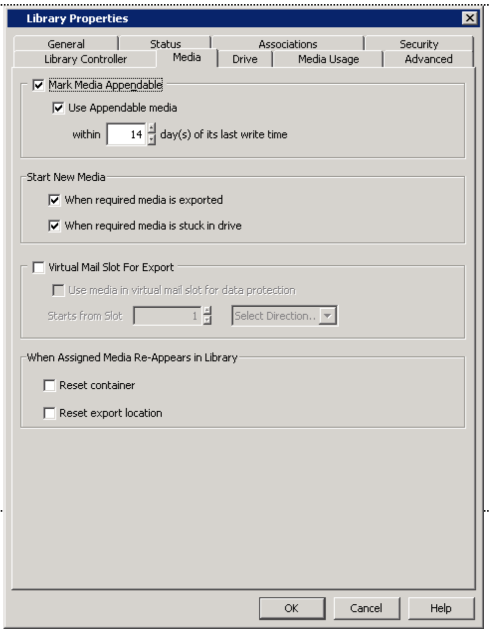
In addition, the number of days within which the appendable media may be re-used can also be specified. Specifying the number of days prevents data belonging to backup cycles from being fragmented across several media, which also facilitates pruning of data and recycling of media in the library. Consider the following on reusing media that are marked as **Appendable**:

- Media marked as **Appendable** can be re-used only by the storage policy (and the same stream in the storage policy) that was previously used to write to the media.
- Media marked as **Appendable** will be re-used only when the currently **Active** media is either marked as **Full** or not available in the library.
- **Appendable** media will not be reused if an **Active** media was marked **Full** by a Synthetic Full backup.

By default, the **Use Appendable Media** option is enabled for 14 days for a library.

A media can also be marked as **Appendable** by the system under certain conditions. For a detailed explanation on when a media is marked as **Appendable**, see Media Status.

See Mark Media as Appendable for step-by-step instructions.



☑ Mark Media Appendable

☑ Use Appendable media

within 14 day(s) of its last write time

Start New Media

☑ When required media is exported

☑ When required media is stuck in drive

☐ Virtual Mail Slot For Export

☐ Use media in virtual mail slot for data protection

Starts from Slot 1 Select Direction...

When Assigned Media Re-Appears in Library

☐ Reset container

☐ Reset export location

SHOW MEDIA RELATED POP-UP MESSAGES ON COMMCELL CONSOLE

On stand-alone drives, to ensure that jobs have the appropriate media in place, pop-up messages are displayed when a wrong media or no media is available in the drive. These pop-up messages are displayed in the MediaAgent computer. You can enable this option to display the message in both the MediaAgent computer and the CommCell Console (irrespective of where it is open). See Pop-up Messages in Stand-Alone Drives for more information.

AUTOMATICALLY USE SPARE MEDIA FROM DIFFERENT SCRATCH POOL IF FOUND

On stand-alone drives, when this option is enabled, the system will use a spare media from another scratch pool if the media is available in the drive.

Enabling this option ensures that data protection operations (and other write operations) continue smoothly when the media from the specific scratch pool is not available for the job. If this option is not enabled, the job will remain in the **Waiting** state, until the media from the specific scratch pool is made available in the drive. Appropriate Event messages are displayed in the **Event Viewer**. See Detecting Media Changes in Stand-Alone Drives for more information.

By default the **Automatically use spare media from different scratch pool if found in drive** option is enabled for stand-alone drives.

UNLOAD MEDIA IN STANDALONE DRIVE WHEN MEDIA IS REQUIRED

On stand-alone drives, when this option is enabled, the system will automatically unload the media from the drive when a different media is required. (If the stand-alone drive supports the automatic ejection of the media from the drive, the media will also be ejected.)

If this option is not selected, the system will not unload the media from the drive and will overwrite the media (when a job is initiated) if the **Overwrite Media in drive if Media Not Written to in (n) Days/Hours** is enabled, after the time specified in this option. See Media Operations in Stand-Alone Drives for more information.

By default the **Unload media in standalone drive when different media is required** option is enabled for stand-alone drives.

START NEW MEDIA

When the **Assigned** media is not available, either because it was exported or stuck in the drive, a new media can be used for the job by enabling the **When required media is exported** and **When required media is stuck** options.

Enabling these options ensure that data protection operations continue smoothly when the required media is not available for the job. If these options are not enabled, the job will remain in the **Waiting** state, until the assigned media is made available, either by importing or after it is manually loaded in the drive. Appropriate Event messages are displayed in the **Event Viewer**. See Start New Media for Data Protection Operations when Media is Exported and Start New Media for Data Protection Operations when Media is Stuck for step-by-step instructions.

By default the **Start New Media** options are enabled for a library.

Another form of Start New Media option is also available for Data Protection and Auxiliary Copy jobs. See Advanced Backup/Migrate/Archive Options - Start New Media for more information.

BARCODE LABELING SCHEME

The options in this area provide you the ability to customize the media labels for stand-alone drives and blind libraries. (See Media Labeling in Stand-Alone Drives and Media Labeling in Blind Libraries for additional details.)

VIRTUAL MAIL SLOT FOR EXPORT

Virtual Mail Slots are use by Vault Tracker to store the media in a range of contiguous slots in the library. For comprehensive information on Vault Tracker, see Vault Tracker.

The media options for a library can be viewed or modified from the **Media** tab of the **Library Properties** dialog box.

See Set up the Virtual Mail Slots in the Library for step-by-step instructions.

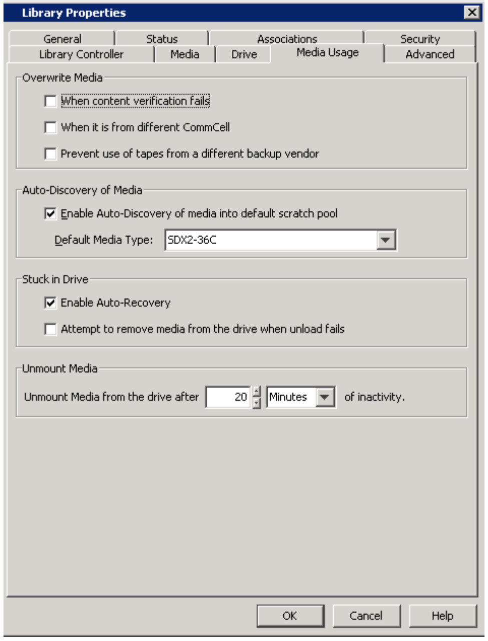
WHEN ASSIGNED MEDIA RE-APPEARS IN LIBRARY

The options in this area is useful to globally reset the container and/or export location associations for media, when a media is recalled or re-imported back to a library. These associations are viewable from the Media Properties - General tab. By default, these options are not enabled for a library. (See Recall Media, Export Media and Import Media for more information on the specific operation.)

See Reset Container and Export Media Location for Media in the Library for step-by-step instructions.

MEDIA USAGE

OVERWRITE MEDIA



Overwrite Media

☐ When content verification fails

☐ When it is from different CommCell

☐ Prevent use of tapes from a different backup vendor

Auto-Discovery of Media

☑ Enable Auto-Discovery of media into default scratch pool

Default Media Type: SDX2-36C

Stuck in Drive

☑ Enable Auto-Recovery

☐ Attempt to remove media from the drive when unload fails

Unmount Media

Unmount Media from the drive after 20 Minutes of inactivity.

- A media can be automatically overwritten when an error is encountered while reading the on media label (OML) by enabling the **When Content Verification Failed** option. If this option is not enabled, a mount error is displayed in the **Event Viewer**, when an error is encountered while reading the OML.

  Caution should be exercised while enabling this option, as a valid media can be over written in certain cases. It is recommended that you enable this option to just overwrite a media that you know for certain can be overwritten. Once the specific media is overwritten, disable the option.

  > **WARNING**
  >
  > If this option is enabled and if a valid media with a different barcode is mounted by mistake, data in the valid media will be overwritten.

- Media containing data from other CommCells can be overwritten by enabling the **When it is from a different CommCell** option. If this option is not enabled, such media will be marked as **Bad** and moved to the **Retired Media** group. A mount error is displayed in the **Event Viewer**, indicating that the media is from another CommCell.
- On stand-alone drives, to facilitate the availability of media for data protection operations, you can enable the **Overwrite Media if Media Last Written to in (n) Days/Hours** option. This ensures that older media is used by the operation when a spare media or media marked as **Appendable** is not available in the library.

  By default the **Overwrite Media** options are disabled for a library.

  > **WARNING**
  >
  > It is strongly recommended that this option be disabled at all times to prevent over-writing of data available in the media.
  >
  > Do not enable this option on a library with mixed drive types.

See Overwrite Media with Old Data When Spare or Appendable Media is Unavailable for step-by-step instructions.

PREVENT USE OF TAPES FROM A DIFFERENT BACKUP VENDOR

This option can be used on libraries that are shared between different backup vendors. When this option is enabled the MediaAgent will automatically prevent the usage of media associated with other backup vendors. By default this option is not enabled. Note that this option will be available only if the option to overwrite media **When Content Verification Failed** option is disabled.

> As each backup vendor has a unique method of writing data on a media, the system can identify the media associated with specific backup vendors. Contact your software provider to obtain the list of supported backup vendors.

AUTO-DISCOVER OF MEDIA

- **ENABLE AUTO-DISCOVER MEDIA INTO DEFAULT SCRATCH POOL**

  When this option is enabled, new media is automatically discovered whenever you import or introduce new media to the library. The new media is automatically moved to the default scratch pool.

  If the option is not enabled, media must be manually discovered.

  You can either enable or disable this option by default, during the library configuration process.

  You can also enable the automatic discovery for cleaning media.

  For comprehensive information on discovering media, see Discover Media.

- **ONLY USE PNP DISK WHEN IT IS BLANK**

  Enabling this option ensures that blank disks with no other data is used for data protection operations and allows you to use disks exclusively for data protection purposes. (See Enable (or Disable) Option to Only Use Blank PnP Disks for step-by-step instructions.)

- **USE DISK ONLY WHEN THE SIZE IS GREATER THAN (N) MB**

  Enabling this option and specifying the minimum disk size ensures that data protection operations use disks with a specific size. Depending on the size of your data protection operations, you can avoid using smaller disks which may result in a job spanning multiple disks.

See Enable (or Disable) Automatic Media Discovery for step-by-step instructions.

AUTO STAMP MEDIA IN DRIVE

On stand-alone drives, when this option is enabled, the system automatically stamps a new label when an unidentified (or new) media is loaded in the drive. The system uses the specified Barcode Labeling Scheme or a default label to stamp the media. (See Media Labeling in Stand-Alone Drives for additional details.)

STUCK IN DRIVE

ENABLE AUTO-RECOVERY

The MediaAgent will attempt to recover media, that may be stuck in a drive, if the **Enable Auto-Recovery** option is enabled. By default this option is enabled. By default the MediaAgent tries to recover the media from the drive every 20 minutes. You can modify the frequency using the nAUTOSTUCKTAPERECOVERYINTERVALMIN registry key.

By default, the **Enable Auto-Recovery** option is enabled in the library.

ATTEMPT TO REMOVE MEDIA FROM THE DRIVE WHEN UNLOAD FAILS

Similarly, the MediaAgent will use the move command to unmount media when the unload command in a drive fails if the **Attempt to remove media from the drive when unload fails** option is enabled.

You may want to enable this option if your library supports options to unload drive as a part of the move command.

By default, the **Attempt to remove media from the drive when unload fails** option is disabled in the library.

If the above options are not enabled, the drive status is displayed as **offline**, when a job encounters a stuck media or is unable to unmount the media from the drive. In such a situation, you must manually recover the media from the drive and then mark the drive online.

See Enable (or Disable) Stuck Media Recovery for step-by-step instructions.

UNMOUNT MEDIA

The system automatically unmounts media that remain idle in the drive. This option allows you to specify the idle time after which the media should be unmounted from the drive.

In regular libraries, the media will be automatically unloaded when the media remains idle for the specified amount of time.

In stand-alone libraries the media will either be ejected from the drive or remain in the drive in the unloaded state (depending on the drive type) when the media remains idle for the specified amount of time. See Media Operations in Stand-Alone Drives for more information.

DRIVE

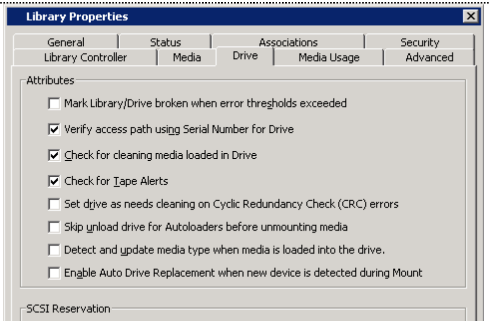
ATTRIBUTES

MARK LIBRARY/DRIVE BROKEN WHEN ERROR THRESHOLDS EXCEEDED

When a library exceeds the threshold values established for the library type in the Hardware Maintenance for a library, or when a drive in the library exceeds the threshold values established for the drive type, the system will mark them as Broken if you enable the **Mark Library/ Drive Broken When Error Thresholds Exceeded** option. By default the **Mark Library/Drive Broken When Error Thresholds Exceeded** option is disabled for a library.

VERIFY ACCESS PATH USING SERIAL NUMBER OF DRIVE

Enabling this option ensures that the drive serial number and access paths are verified before reading or writing to the media. It is strongly recommended that this option be enabled at all times to prevent the overwriting of data, when the drive access path is changed due to hardware configuration changes.



Attributes

☐ Mark Library/Drive broken when error thresholds exceeded

☑ Verify access path using Serial Number for Drive

☑ Check for cleaning media loaded in Drive

☑ Check for Tape Alerts

☐ Set drive as needs cleaning on Cyclic Redundancy Check (CRC) errors

☐ Skip unload drive for Autoloaders before unmounting media

☐ Detect and update media type when media is loaded into the drive.

☐ Enable Auto Drive Replacement when new device is detected during Mount

SCSI Reservation

By default, the **Verify access path using Serial Number of Drive** option is enabled in the library.

See Enable (or Disable) the Verification of Drive Access Path and Serial Number for step-by-step instructions.

CHECK FOR CLEANING MEDIA LOADED IN DRIVE

When this option is enabled, the system always checks the media to see if it is a cleaning media, before performing any other operation on the media.

By default, the **Check for cleaning media loaded in Drive** option is enabled in the library.

> It is strongly recommended that this option be enabled at all times. In most libraries, unselecting this option may result in SCSI failures which requires manual intervention to unload the cleaning media from the drive.

See Enable (or Disable) the Checking for Cleaning Media Loaded in the Drive for step-by-step instructions.

CHECK FOR TAPE ALERTS

When this option is enabled, the system logs the drive errors (provided by the hardware manufacturers) while the drive is in use. The drive errors are logged into **CVMA.log** and **CVD.log** and can be used for troubleshooting the drive. By default, the **Check for Tape Alerts** option is enabled in the library.

See Enable (or Disable) the Logging of Tape Alerts for step-by-step instructions.

SET DRIVE AS NEEDS CLEANING ON CYCLIC REDUNDANCY CHECKS (CRC) ERRORS

When this option is enabled, the system automatically marks the drive as Requires Cleaning when drive reports CRC errors during read/write operations.

SKIP UNLOAD DRIVE FOR AUTOLOADERS BEFORE UNMOUNTING MEDIA

When this option is enabled, the MediaAgent skips the unload operation before unmounting the media from the drive. This can be enabled for libraries with autoloaders that automatically perform the unmount operation while unloading media. Typically you can enable this option on libraries, where unmount operations constantly fail with the error `Operation failed as the source is empty`. By default this option is not enabled.

DETECT AND UPDATE MEDIA TYPE WHEN MEDIA IS LOADED INTO THE DRIVE

When this option is enabled, the MediaAgent automatically detects the correct media type when the media is used the first time. For example, if you import mixed media in bulk and discovered them as a specific media type. (The media type information can be viewed from the **Media Properties** associated with the specific media.) This option is supported for IBM Ultrium and DLT/SDLT drives. By default this option is not enabled.

ENABLE AUTO DRIVE REPLACEMENT WHEN NEW DEVICE IS DETECTED DURING MOUNT

When this option is enabled, the MediaAgent automatically detects and update information pertaining to new drives that were replaced, during a subsequent mount operation. This option is supported on libraries that support drive serialization and also when a drive is replaced with the same drive type. It is strongly recommended that this option be enabled before replacing drives in libraries that support drive serialization as it provides a one touch solution for replacing drives. In some cases the system may not automatically detect the new drives. In such situations, follow the alternate procedures described in Hardware Changes to replace the drives. By default this option is not enabled.

See Automatically Detect Replaced Drives for step-by-step instructions.

For STK libraries attached to ACSLS Server, you can enable the **Use Drive ID for Drive Replacement** in the **Library Properties** dialog box.

CHECK FOR MEDIA CHANGE IN DRIVE EVERY N MINUTES

On stand-alone drives, when this option is enabled, the system automatically check the media in the drive to update the media information based on the specified minutes. See Detecting Media Changes in Stand-Alone Drives for additional details.

SCSI RESERVATION

Enabling SCSI reservation prevents multiple MediaAgent hosts within a SAN environment from accessing the same drive concurrently. This option, when enabled, prevents the risk of data corruption by ensuring that the initiating MediaAgent has use of the drive exclusively during data protection and other operations. This option is useful in the SAN environment where multiple computers may try to access the same drive, resulting in data corruption.

Refer to the hardware manufacturer's documentation to determine if the target device supports SCSI-2 or SCSI-3 reservation. Enabling a SCSI standard that is not supported by the hardware may result in data protection job failures.

Both SCSI-2 and SCSI-3 reservations are supported. If supported across all Hardware, SCSI-3 would be the preferred setting. SCSI-3 has added benefits of Persistent Reservation features and preempting abilities. Before enabling either option, ensure the following:

- Verify that the target device supports either SCSI-2 or SCSI-3 command set for persistent reservation. Most tape drives are known to support either of these command sets.
- Inter-connecting hardware, such as storage routers or bridge, which connects standard SCSI devices into FC fabric, should also support this command. If you encounter any differences in behavior with this command, then identify the differences in the interconnecting components from the working host to non-working host. (Refer to the hardware manufacturer's documentation to see if this operation is supported.)
- When using SCSI-3 command set, make sure that the device drivers for the target device do not perform an implicit reservation. Some of drivers in Windows as well as on Unix are known to perform SCSI-2 reservation implicitly when the device handle is opened by an application. In this case the SCSI-3 reservation will fail with *Reservation conflict*, as SCSI-2 reservation is already active in the target. (Check the driver's behavior using the documentation provided for the driver.) Notably, some IBM LTO family drivers and STK 9x40 family drivers are known to perform SCSI-2 reservation on Windows. On Unix, there are hooks to enable implicit reservation using a known interface through native drivers.

  Use the **ScsiCmdTool** to test whether the hardware supports SCSI-3 reservation. See ScsiCmd Tool for more information.

This feature requires a Feature License to be available in the CommServe® Server.

Review general license requirements included in License Administration. Also, View All Licenses provides step-by-step instructions on how to view the license information.

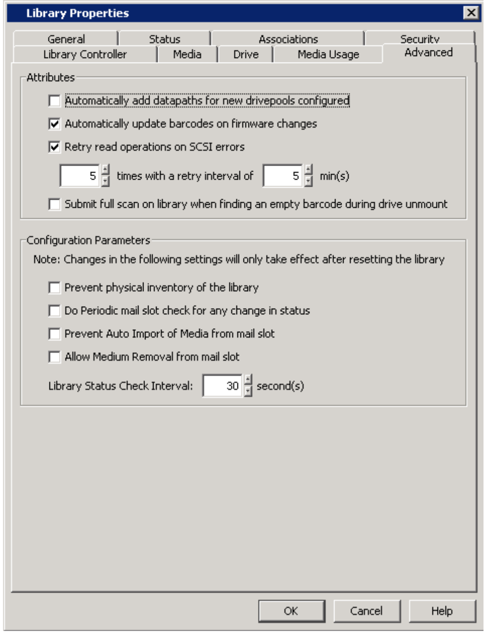
SCSI-2 reservation is enabled by default for all tape drives attached to a newly installed MediaAgent in this release. When you upgrade a MediaAgent, SCSI-3 reservation will be enabled if it was enabled in the previous release. If SCSI-3 was not enabled, the SCSI reservation itself (which includes both SCSI-2 and SCSI-3 reservation) is disabled.

ENABLE AUTO-CLEANING

When these options are enabled, the cleaning tape is automatically mounted and a cleaning operation is initiated on the drive, whenever the selected options indicate that the drive requires cleaning. For comprehensive information on drive cleaning, see Drive Cleaning.

ADVANCED

ATTRIBUTES



Attributes

☐ Automatically add datapaths for new drivepools configured

☑ Automatically update barcodes on firmware changes

☑ Retry read operations on SCSI errors

5 times with a retry interval of 5 min(s)

☐ Submit full scan on library when finding an empty barcode during drive unmount

Configuration Parameters

Note: Changes in the following settings will only take effect after resetting the library

☐ Prevent physical inventory of the library

☐ Do Periodic mail slot check for any change in status

☐ Prevent Auto Import of Media from mail slot

☐ Allow Medium Removal from mail slot

Library Status Check Interval: 30 second(s)

AUTOMATICALLY ADD DATAPATHS FOR NEW DRIVEPOOLS CONFIGURED

When enabled, the system automatically adds the alternate data paths for a shared library. It is also essential to enable the following option in the storage policy copy properties for this option to work: **Automatically add new datapath** option in the **Copy Properties (Data Paths)** tab.

This option can be used when several MediaAgents share a library. This will help you to automatically create alternate data paths in the associated storage policy during the library configuration.

AUTOMATICALLY UPDATE BARCODES ON FIRMWARE CHANGES

When a library's firmware is upgraded or when a hardware is replaced, sometimes it would start reading the barcodes of the media in the library differently by appending, pre-pending or truncating some characters in the barcode. When this option is enabled the system automatically updates the media barcodes in the library - both media inside the library and exported media. By default this option is enabled in the library.

Note the following assumptions:

- The length of the barcode for all media inside the library is the same.
- When the firmware is changed, the new string which is appended, pre-pended or truncated is the same for all the media. For example:

  Old Barcodes

  000012

  000013

  New Barcodes

  000012L1

  000013L1
- There will be a difference in the length of the old barcodes and new barcodes.

If this option is disabled, and the barcodes are changed after a firmware upgrade all existing media, including media with data and spare media will be marked as exported and a new set of media (with new barcodes) will be listed inside the library. In this situation, you must update the barcodes as described in Manually Updating Media Barcodes after a Firmware Upgrade.

RETRY READ OPERATIONS ON SCSI ERRORS

This option indicates whether the MediaAgent will reposition the tape and retry the read operation (*i.e.*, data recovery operation, auxiliary copy operation, synthetic full job, etc) on SCSI errors, to prevent the failure of the job. You can also indicate how many times and how often the retry must be attempted.

By default the **Retry read operations on SCSI errors** option is enabled and the system tries to retry 5 times every 5 minutes.

SUBMIT FULL SCAN ON LIBRARY WHEN FINDING AN EMPTY BARCODE DURING DRIVE UNMOUNT

Indicates whether a full scan of the library will be performed when an empty barcode is found while unmounting the drive. This is a troubleshooting option which can be enabled in a library if you constantly find that the system indicates that the media is exported when requested by a job, but physically found in the library. For the specific job to succeed, you must perform a full scan of the library. But if you find the problem occurring frequently you can enable this option. By default this option is not enabled.

CONFIGURATION PARAMETERS

The following parameters can be established under certain conditions based on the library. Note that changes to any of these parameters will take effect only when the library is Reset.

PREVENT PHYSICAL INVENTORY OF THE LIBRARY

This option provides the facility to disable the full scan operation initiated by the MediaAgent when there is a unit attention. (i.e., when the door is accessed, the mail slot is accessed, the library controller is reset, etc.)

In some older libraries, the firmware itself automatically initiates an inventory when there is a unit attention. If you notice that there is a double scan of the library after a unit attention, you can enable this option.

By default, the **Prevent physical inventory of the library** option is disabled.

DO PERIODIC MAIL SLOT CHECK FOR ANY CHANGE IN STATUS

When this option is enabled, the MediaAgent will poll the library to see if there is any change in the status of the mail slot. Enable this option in libraries that do not automatically generate unit attention when there is a change in the mail slot. For example, when media is imported or exported and the mail slot is accessed to add or remove the media, the system will never know the status of the operation, unless this option is enabled. You can also specify how often the library must be polled by setting the **Library Status Check Interval**.

By default, the **Do Periodic mail slot check for any change in status** option is disabled.

PREVENT AUTO IMPORT OF MEDIA FROM MAIL SLOT

When this option is enabled, media will not be automatically moved from the mail slot into the library. Instead the media will be moved only when an import operation is initiated from the CommCell Console.

We recommend that you enable both the **Prevent Auto Import of Media from mail slot** and **Do Periodic mail slot check for any change in status** options if you have a library which is partitioned into two or more logical partitions and the mail slot is shared by these logical libraries. This will ensure that the media is imported (or exported) to the appropriate library.

This option is also useful to control the import media operation using only the CommCell Console.

By default, the **Prevent Auto Import of Media from mail slot** option is disabled.

ALLOW MEDIUM REMOVAL FROM MAIL SLOT

When this option is enabled, the library handler will issue a SCSI command during startup to unlock the library mail slot. By default this option is not enabled.

This option is useful when other software may lock the library mail slot and you would like the mail slot to be opened.

LIBRARY STATUS CHECK INTERVAL

This option indicates how often the MediaAgent must poll the library to see if there is a change in the status of the library such as a change in the status of the mail slot, library door, library connectivity to the Media Agent, etc.

If the **Do Periodic mail slot check for any change in status** option is enabled, this interval also indicates how often the MediaAgent polls the library to see if there is a change in the status in the mail slot.

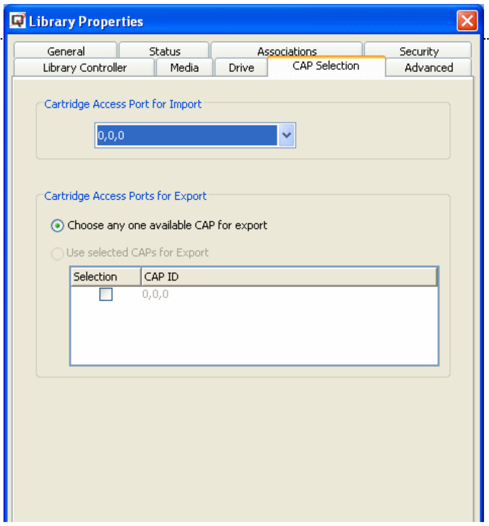
CAP SELECTION

The following CAP Selection options can be established for the libraries attached to ACSLS Servers:

CARTRIDGE ACCESS PORT FOR IMPORT AND EXPORT

If you have multiple mail slots in the library, the CAP ID associated with the mail slot that will be used for importing and exporting the media used by the specific MediaAgent. If necessary, you can also change the CAP ID if the specified CAP is busy.

See Best Practices for STK Libraries Attached to ACSLS Server for more information.



Cartridge Access Port for Import: 0,0,0

Cartridge Access Ports for Export

● Choose any one available CAP for export

○ Use selected CAPs for Export

Selection	CAP ID
□	0,0,0

OTHER CONSIDERATIONS

AUDIT TRAIL

Operations performed with this feature are recorded in the Audit Trail. See Audit Trail for more information.

Back To Top

Library Properties - How To

Topics | How To | Related Topics

General

- Change the Default Scratch Pool
- Modify the Mount and Unmount Timeouts

Status

- Enable (or Disable) the Library
- View the Library Offline Reason
- Mark MediaAgent/Library/Drive Offline for Maintenance

Associations

- View the Storage Policies Accessing a Library

Library Controller

- Change the Active Library Controller
- View the Status of the Library Controller

Media

- Mark Media as Appendable
- Reuse Media Marked as Appendable
- Start New Media for Data Protection Operations when Media is Exported
- Start New Media for Data Protection Operations when Media is Stuck
- Set up the Virtual Mail Slots in the Library
- Enable (or Disable) Media Related Pop-Ups in the CommCell Console
- Enable (or Disable) Automatic Use of Spare Media from Different Scratch Pools
- Enable (or Disable) Unloading of Media from a Stand-alone Drive when Different Media is Required
- Reset Container and Export Media Location for Media in the Library
- Modify the Barcode and Location for a Media Associated with a Stand-Alone Drive

Media Usage

- Overwrite Media with Old Data When Spare or Appendable Media is Unavailable
- Enable (or Disable) Automatic Media Discovery
- Enable (or Disable) Stuck Media Recovery
- Modify the Unmount Time for Inactive Media in the Drive
- Reuse Media with Failed Content Verification
- Enable Usage of Media From Other CommCells

Drive

- Enable (or Disable) the Verification of Drive Access Path and Serial Number
- Enable (or Disable) the Checking for Cleaning Media Loaded in the Drive
- Enable (or Disable) the Logging of Tape Alerts
- Automatically Detect Replaced Drives

CAP ID

- Specify the CAP ID for Importing and Exporting Media

CHANGE THE DEFAULT SCRATCH POOL

Required Capability: See Capabilities and Permitted Actions

To change the default scratch pool:

1. From the CommCell Browser, right-click the library for which you wish to change the default scratch pool, and then click **Properties**.
2. Select the name of the scratch pool that you wish to designate as the default scratch pool from the **Default Scratch Pool** list.
3. Click **OK** to save the changes.

MODIFY THE MOUNT AND UNMOUNT TIMEOUT PERIODS

Required Capability: See Capabilities and Permitted Actions

To modify the mount and unmount timeout periods:

1. From the CommCell Browser, right-click the library for which you wish to change mount and unmount timeout periods, and then click **Properties**.
2. In the **Mount** and **Unmount** box, type or select the timeout periods.

3. Click **OK** to save the changes.

Enable (or Disable) the Library

Required Capability: See Capabilities and Permitted Actions

To enable or disable a library:

1. From the CommCell Browser, right-click the library you wish to enable or disable, and then click **Properties**.
2. Click the Status tab.
3. In the **Status** area, click **Enable Library**.
4. Click **OK** to save the changes.

View the Library Offline Reason

Required Capability: See Capabilities and Permitted Actions

To view the offline reason for a library:

1. From the CommCell Browser, right-click the library for which you wish to view the offline reason, and then click **Properties**.
2. Click the Status tab.
3. Information on the library offline reason is displayed in the **Offline Reason** box.

Mark MediaAgent/Library/Drive Offline for Maintenance

Required Capability: Capabilities and Permitted Actions

To mark MediaAgent/Library/Drive Offline for Maintenance:

1. From the CommCell Browser, right-click the MediaAgent/Library/ Drive that you wish to mark offline for maintenance, and then click **Properties**.
2. Select one or more of the following options as appropriate:
   - To mark a MediaAgent offline for maintenance: Click the Control tab and then click and enable the **Mark MediaAgent Offline for Maintenance** option.
   - To mark a library offline for maintenance: Click the Status tab and then click and enable the **Mark Library Offline for Maintenance** option.
   - To mark a drive offline for maintenance: Click the Status tab and then click and enable the **Mark Drive Offline for Maintenance** option.
3. Click **OK** to save the configuration.

   Subsequent data protection, data recovery and auxiliary copy operations will not use the associated MediaAgent/Library/Drive.

View the Storage Policies Accessing a Library

Required Capability: See Capabilities and Permitted Actions

To view the storage policies accessing a library:

1. From the CommCell Browser, right-click the library for which you wish to view the storage policies, and then click **Properties**.
2. Click the Associations tab.

   All the storage policies and storage policy copies accessing the library are displayed.

Change the Active Library Controller

Use the following procedure to manually switch the active library controller in a library configured with library controllers, in the SAN environment.

Before You Begin

- Do not switch the active library controller if jobs are in progress for that MediaAgent

Required Capability: See Capabilities and Permitted Actions

To change the active library controller:

1. From the CommCell Browser, right-click the library for which you wish to change the active library controller, and then click **Properties**.
2. Click the Library Controller tab.
3. Click **Change**.
4. In the Change Active Library Controller dialog box, choose the library controller that you wish to designate as the active library controller from the **Failover Controllers** list.

   In order to manually change a failover library controller candidate as the active library controller, the failover library controller candidate must be **Alive** and **Enabled**.

5. Click **OK** in both the **Change Active Library Controller** dialog box and in the **Library Properties** dialog box.

   The selected failover library controller is switched as the active library controller.

View the Status of the Library Controller

Required Capability: See Capabilities and Permitted Actions

To view the status of the library controller:

1. From the CommCell Browser, right-click the library for which you wish to view the library controller status, and then click **Properties**.
2. Click the Library Controller tab.

   The status of the library controller can be viewed in the **Library Properties (Library Controller)** dialog box. Note the following:

   The **Active Library Controller** is the MediaAgent with the **Active**, **Alive** and **Enabled** status as *YES*, and the **Soft State** as *ON*. (You can view the status of the library controllers by clicking the **Detail** button on the **Active Library Controller** or **Failover Library Controller** panes.)

   - In a library configured in the SAN environment, where several MediaAgents are configured as library controllers, at any given point, the MediaAgent accessing the library is considered as **Active** and therefore displayed as the Active Library Controller. All the other MediaAgents are displayed as **Failover Library Controllers**. The **Active** status will be displayed as *No* for the failover library controllers.
   - In a library configured in the non-SAN environment, where only one MediaAgent is configured as a library controller, the MediaAgent is displayed as the Active Library Controller. If either the Alive or Enabled status is NO, or Soft State is OFF, the Active status will be displayed as OFF and the MediaAgent will be displayed as a **Failover Library Controller**.

Mark Media as Appendable

Required Capability: See Capabilities and Permitted Actions

To mark media as appendable:

1. From the CommCell Browser, right-click the library for which you wish to mark the media as appendable, and then click **Properties**.
2. Click the Media tab.
3. Click **Mark Media Appendable**.
4. In the **Use Appendable Media within n Day (s) of its last write time,** type the number of days that the media can be used after it was marked as appendable.
5. Click **OK** to save the changes.

Reuse Media Marked as Appendable

Required Capability: See Capabilities and Permitted Actions

To reuse media marked as appendable:

1. From the CommCell Browser, right-click the library for which you wish to reuse media marked as appendable, and then click **Properties**.
2. Click the Media tab.
3. Click **Use Appendable Media within n Day (s) of its last write time**.
4. Type the number of days that the media can be used after it was marked as appendable.
5. Click **OK** to save the changes.

Start New Media for Data Protection Operations when Media is Exported

Required Capability: See Capabilities and Permitted Actions

To start new media for data protection operations, when the required media is exported:

1. From the CommCell Browser, right-click the library for which you wish to start new media for data protection operations, when the required media is exported, and then click **Properties**.
2. Click the Media tab.
3. From the **Start New Media** region, click **When required media is exported**.
4. Click **OK** to save the changes.

Start New Media for Data Protection Operations when Media is Stuck

Required Capability: See Capabilities and Permitted Actions

To start new media for data protection operations, when the required media is stuck:

1. From the CommCell Browser, right-click the library for which you wish to start new media for data protection operations, when the required media is stuck, and then click **Properties**.
2. Click the Media tab.
3. From the **Start New Media** region, click **When required media is stuck**.
4. Click **OK** to save the changes.

Set up the Virtual Mail Slots in the Library

Required Capability: See Capabilities and Permitted Actions

To setup the virtual mail slots in the library:

1. From the CommCell Browser, right-click the library for which you wish to setup the virtual slots, and then click **Properties**.
2. Click the Media tab.
3. Click the **Virtual mail slot for export** option.
4. Enter the starting slot number that must be used for storing media in the virtual mail slot in the **Starts From** box.
5. Specify whether the direction that must be used from the starting slot number. (The options are UP and Down.)
6. Click **OK** to save the information.

To use the virtual mail slot, the VaultTracker job must have the Use Virtual Mail Slot option enabled. You can enable this option in one of the following dialog boxes:

- Selecting the **Use Virtual Mail Slots for export in source libraries** option in the Tracking Policy from the Tracking Policy Details (Criteria) dialog box.
- Selecting the **Use Virtual Mail Slots** option for a backup job, from the **Advanced Backup Options** dialog box.
- The MediaAgent does not support the creation of virtual mail slots for blind libraries and libraries attached to an ACSLS server.

Enable (or Disable) Media Related Pop-Ups in the CommCell Console

Related Topics:

- Pop-up Messages in Stand-Alone Drives

Required Capability: See Capabilities and Permitted Actions

To enable (or disable) media related pop-ups in the CommCell Console:

1. From the CommCell Browser, right-click the library for which you wish to enable or disable the pop-ups then click **Properties**.
2. Click the Media tab.
3. Click on **Show Media related pop-up messages on CommCell Console** to enable the option, or clear the option to disable it.
4. Click **OK** to save the changes.

Enable (or Disable) Automatic Use of Spare Media from Different Scratch Pools

Required Capability: See Capabilities and Permitted Actions

To enable (or disable) automatic use of spare media from different scratch pools:

1. From the CommCell Browser, right-click the library for which you wish to enable or disable this option then click **Properties**.
2. Click the Media tab.
3. Select the **Automatically use spare media from different scratch pool if found in drive** to enable the option, or clear the option to disable it.
4. Click **OK** to save the changes.

Enable (or Disable) Unloading of Media From a Stand-Alone Drive When Different Media is Required

Required Capability: See Capabilities and Permitted Actions

To enable (or disable) unloading of media from a stand-alone drive when different media is required:

1. From the CommCell Browser, right-click the library for which you wish to enable or disable this option then click **Properties**.
2. Click the Media tab.
3. Select the **Unload media in standalone drive when different media is required** to enable the option, or clear the option to disable it.
4. Click **OK** to save the changes.

Reset Container and Export Media Location for Media in the Library

Required Capability: See Capabilities and Permitted Actions

To reset container and export media location for media in the library:

1. From the CommCell Browser, right-click the library you wish to reset the container and/or export media location, and then click **Properties**.
2. Click the Media tab.
3. In the **When Assigned Media Re-Appears in Library** area, select the **Reset container** and/or **Reset export location** options to enable them:
4. Click **OK** to save the changes.

Modify the Barcode and Location for a Media Associated with a Stand-Alone Drive

Required Capability: See Capabilities and Permitted Actions

To modify the barcode and location for a media associated with a stand-alone drive

1. From the CommCell Browser, click on **Exported Media** or **Assigned Media** group associated with a stand-alone drive in which the media is available. All the media existing in the stand-alone drive are displayed on the right-pane of the CommCell browser
2. Right-click the media for which you want to modify the properties, and then click **Properties**.
3. In the **Barcode/ Identifier** box, type a new barcode/identifier for the media.
4. In the **Location** box, type the location in which the media is stored.
5. Click OK to save the changes.

Overwrite Media with Old Data, When Spare or Appendable Media is Unavailable

Required Capability: See Capabilities and Permitted Actions

To overwrite media with old data, when Spare or Appendable media is unavailable in the library:

1. From the CommCell Browser, right-click the library in which you wish to enable this option, and then click **Properties**.
2. Click the Media Usage tab.
3. Click **Overwrite Media if Media Last Written to in**.
4. Type the number of days/hours after which the media can be reused.

5. Click **OK** to save the changes.

Enable or Disable Automatic Media Discovery

Required Capability: See Capabilities and Permitted Actions

To enable automatic media discovery:

1. From the CommCell Browser, right-click the library for which you wish to enable automatic media discovery, and then click **Properties**.
2. Click the Media Usage tab.
3. From the **Auto-Discovery of Media** region, click **Enable Auto-Discovery of Media into default scratch pool** option. (Clear this check box to disable this option.)
4. Select the default media type available in the library from the **Default Media Type** list.

   Note that the media available in a library must be compatible with the drives attached to the library.
5. Click **OK** to save the changes.

   When you subsequently import media, the imported media is automatically moved to the default scratch pool.

Enable or Disable Stuck Media Recovery

Required Capability: See Capabilities and Permitted Actions

To enable or disable stuck media recovery:

1. From the CommCell Browser, right-click the library for which you wish to enable or disable stuck media recovery, and then click **Properties**.
2. Click the Media Usage tab.
3. From the **Stuck in Drive** region, choose the necessary options. (Clear the appropriate check boxes to disable this option.)
4. Click **OK** to save the changes.

Modify the Unmount Time for Inactive Media in the Drive

Required Capability: See Capabilities and Permitted Actions

To modify the unmount time for inactive media in the drive:

1. From the CommCell Browser, right-click the library for which you wish to modify the unmount time for inactive media in the drive, and then click **Properties**.
2. Click the Media Usage tab.
3. From the **Unmount Media from the drive after (n) Minutes/Hours of inactivity** box, type the unmount time that you wish to establish and then choose minutes or hours.
4. Click **OK** to save the changes.

Reuse Media with Failed Content Verification

Required Capability: See Capabilities and Permitted Actions

Use the following procedure to overwrite media in situations where the MediaAgent fails to read a media, e.g., incompatible data formats, etc.

To reuse media with failed content verification:

1. From the CommCell Browser, right-click the library for which you wish to reuse media with failed content verification, and then click **Properties**.
2. Click the Media tab.
3. From the **Overwrite Media** region, click **When Content Verification Failed.**
4. Click **OK** to save the changes.

Enable or Disable the Usage of Media From Other CommCells

Use the following procedure to overwrite media from other CommCells.

Required Capability: See Capabilities and Permitted Actions

► To enable or disable the usage of media from other CommCells:

1. From the CommCell Browser, right-click the library for which you wish to enable usage from other CommCells, and then click **Properties**.
2. Click the Media tab.
3. From the **Overwrite Media** region, click **When it is from different CommCell** to enable this option. (Clear this check box to disable this option.)
4. Click **OK** to save the changes.

ENABLE OR DISABLE THE VERIFICATION OF DRIVE ACCESS PATH AND SERIAL NUMBER

Required Capability: See Capabilities and Permitted Actions

► To enable or disable the verification of Drive Access Path and Serial Number:

1. From the CommCell Browser, right-click the library for which you wish to enable or disable this option, and then click **Properties**.
2. Click the Drive tab.
3. From the **Attributes** region, choose the **Verify access path using Serial Number for Drive** to enable this option. (Clear this check box to disable this option.)
4. Click **OK** to save the changes.

ENABLE (OR DISABLE) THE CHECKING FOR CLEANING MEDIA LOADED IN THE DRIVE

Required Capability: Capabilities and Permitted Actions

► To enable or disable the checking for cleaning media loaded in the drive:

1. From the CommCell Browser, right-click the library for which you wish to enable or disable this option, and then click **Properties**.
2. Click the Drive tab.
3. From the **Attributes** region, choose **Check for cleaning media loaded in Drive** to enable this option. (Clear this check box to disable this option.)
4. Click **OK** to save the changes.

ENABLE OR DISABLE THE LOGGING OF TAPE ALERTS

Required Capability: See Capabilities and Permitted Actions

► To enable or disable the logging of tape alerts:

1. From the CommCell Browser, right-click the library for which you wish to enable or disable this option, and then click **Properties**.
2. Click the Drive tab.
3. From the **Attributes** region, choose **Check for Tape Alerts** to enable this option. (Clear this check box to disable this option.)
4. Click **OK** to save the changes.

AUTOMATICALLY DETECT REPLACED DRIVES

Required Capability: See Capabilities and Permitted Actions

► To automatically detect replaced drives:

1. From the CommCell Browser, right-click the library for which you wish to enable the option to automatically detect replaced drives, and then click **Properties**.
2. Click the Drive tab.
3. From the **Attributes** region, choose **Enable Auto Drive Replacement when new device is detected during Mount** to enable this option. (Clear this check box to disable this option.)
4. Click **OK** to save the changes.

NOTES

- This is recommended method for replacing compatible drives as it provides a one touch solution for replacing drives.
- In some cases the system may not automatically detect the new drives. e.g., if the library does not support drive serialization, if the drive is not replaced with a compatible drive type, if the library is attached to a Solaris MediaAgent, etc. In such cases, use one of the following procedures for replacing drives:
  - Replace a Drive with the Same Drive Type
  - Replace a Drive with the Compatible Drive Type
  - Replace a Drive With the Same Drive Type in the SAN DDS Environment
  - Replace a Drive With a Compatible Drive Type in the SAN DDS Environment

SPECIFY THE CAP ID FOR IMPORTING AND EXPORTING MEDIA

Use the following procedure to specify the CAP ID associated with the mail slot that will be used for importing and exporting media from the specific MediaAgent.

Required Capability: See Capabilities and Permitted Actions

To specify the CAP ID for importing and exporting media:

1. From the CommCell Browser, right-click the library for which you wish to change the CAP selection, and then click **Properties**.
2. Click the CAP Selection tab.
3. Select the CAP ID that must be used for importing and exporting media.
4. Click **OK**.

Resource View

The resource view can be used to view the drive and media used by the software at any point in time.

The resource view displays all the drives in the library and the media that is currently used in the drive. The media information includes the barcode\identifier of the media and Job ID associated with the job currently using the media. If the media is not used by a job the resource view displays the Job ID as Ca`che Mounted`.

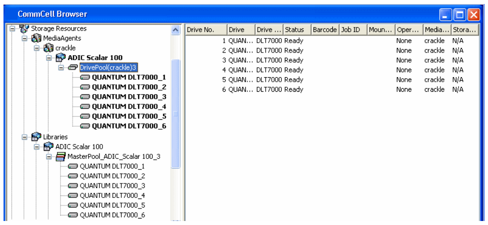
The Resource View includes information on the operation phase to show the specific actions that are occurring on the media in the drive such as writing/verifying/reading OML, loading, unloading, etc.

From the drive level, you can release the reservation on resources, if the reservation is not released when a job has failed or killed in the Job Manager.

In addition, for regular libraries the resource view also displays the slot information in the library and information on media that is currently in the process of being exported.

For Disk libraries, the status and free space information for the mount path is displayed.

The Resource can be viewed from the drive list in the right-pane of the CommCell Browser when you click **Master Drive Pool** or **Drive Pool** in the tree.



Drive No.	Drive	Drive ...	Status	Barcode	Job ID	Moun...	Oper...	Media...	Stora...
1	QUAN...	DLT7000	Ready				None	crackle	N/A
2	QUAN...	DLT7000	Ready				None	crackle	N/A
3	QUAN...	DLT7000	Ready				None	crackle	N/A
4	QUAN...	DLT7000	Ready				None	crackle	N/A
5	QUAN...	DLT7000	Ready				None	crackle	N/A
6	QUAN...	DLT7000	Ready				None	crackle	N/A

Drive Operations

Topics | How To | Troubleshoot | Related Topics

VALIDATE DRIVE

When the drive validation is performed from the CommCell Console, the system performs all the operations that are necessary for operations. This includes, operations such as mounting the media, writing on the media, re-winding and seeking data and then reading back from the media.

It is recommended that a drive validation operation is performed after configuring the libraries and drives and before performing a data protection operation. Drive validation can also be used for troubleshooting purposes. Drive validation can also be performed to check the throughput of the device. In addition, you can verify whether different tape block size is supported by the hardware and operating system, by performing a drive validation operation.

On stand-alone drives, you must have a pre-stamped media available in the drive. Make sure that this pre-stamped media is mounted in the drive and displayed in the CommCell Browser before running the drive validation operation. (You can view the media in the drive using the Resource View.)

Drive validation in not supported for libraries attached to a NAS File Server.

See Validate Drives for step-by-step instructions.

Another form of drive validation can be performed from the **Library and Drive Configuration** window. See Validating Drives in a Library for more details.

MARK DRIVE REPLACED

Sometimes drives must be replaced, either as a result of extended use or because of hardware failure.

> Procedures for replacing drives are hardware specific; refer to the appropriate manufacturer documentation for replacement instructions.

When you have successfully replaced a drive, you must reset all the counters that keep track of the number of drive events. This can be done using the **Mark Drive Replaced** option.

See Mark a Drive as Replaced for step-by-step instructions. For step-by-step instructions on replacing the drive, see Hardware Changes.

MARK DRIVE CLEANED

Use this option to mark a drive as cleaned when you clean the drive manually using the menu options in the library front panel instead of using the Clean Drive option from the CommCell Console.

For a detailed discussion on drive cleaning, see Drive Cleaning.

MARK DRIVE FIXED

If the Mark Library/Drive Broken When Error Thresholds Exceeded option is enabled in the Drive tab of the **Library Properties** dialog box, the status of the drive is marked as **Offline** when the number of hardware errors exceeds the preset threshold values established for the drive. The **Offline Reason** indicates that a threshold was exceeded.

In addition the **Broken** option in the Status tab of the **Drive Properties** is displayed as **Yes**.

In such a situation, it is essential to identify and correct the related problem. Once the problem is addressed, use the **Mark Drive Fixed** option, to remove the broken status and bring the drive **online**. In addition using this option also resets the following counters:

- Number of hard errors since clean
- Number of soft errors since clean

See Mark a Drive as Fixed for step-by-step instructions.

CLEAN DRIVE

Use this option to clean a drive immediately. For a detailed discussion on this option and drive cleaning in general, see Drive Cleaning.

RESET DRIVE

The reset drive option unmounts the media mounted in the drive, thereby making the drive ready for use. The reset drive operation will reset the drive’s status and also try to unmount any media loaded in the drive. However, the reset operation will fail if the drive is reserved or in use.

See Reset a Drive for step-by-step instructions.

UNLOAD DRIVE

Occasionally, hardware errors may cause a media mount failure, making a loaded media inaccessible. When this happens (as indicated in the **Event Viewer**), the affected media must be removed from the drive using the unload drive option. This option can also be used to unmount a loaded free media, when you need to free up the drive immediately for some other use.

See Unload a Drive for step-by-step instructions.

SHOW THROUGHPUT

Drive throughput helps you to calculate and display the drive’s read and write throughput. You can view this information in one of the following ways:

- You can calculate and view the drive throughput for a specified number of hours, using the Show Drive Throughput dialog box.
- You can view a drive’s throughput for the previous hour from the Hardware Info tab of the Drive Properties dialog box.

See View the Drive Throughput for step-by-step instructions.

Drive Operations - How To

Topics | How To | Troubleshoot | Related Topics

CLEAN A DRIVE

Before you Begin

- Do not clean the drive when a job is in progress.
- Ensure that you have imported or moved cleaning media into the Cleaning Media Pool. For more information on importing cleaning media, see Import

Cleaning Media.

- If a job is in progress in the drive you wish to clean, the drive cleaning operation would fail. Ensure that the drive is free, before you start the operation.
- For the MediaAgent to perform the Clean Drive function, the library's auto-cleaning feature must be disabled from the library's front panel menu.

  Refer to the library manufacturer's documentation for information on disabling the library’s auto-clean option from the library’s front panel.

To clean a drive

To clean multiple drives in the library:

1. From the CommCell Browser, right-click the library in which you wish to clean the drives, and then click **Clean Drive**.
2. From the Clean Drive window, click the drives that you wish to clean. (Use CTRL + click to select multiple drives.)
3. Click **OK**.

   You can track the progress of the operation in the Event Viewer.

To clean a specific drive in the library:

1. From the CommCell Browser, right-click the drive you wish to clean, and then click **Clean Drive**.
2. From the Clean Drive window, click **OK.**

   You can track the progress of the operation in the Event Viewer.

NOTES

After the successful completion of the cleaning operation, the counters linked to drive cleaning are reset. You can view these counters from the Drive Properties (Odometers) tab.

VIEW THE DRIVE THROUGHPUT

To calculate the drive throughput for a specified time

1. In the CommCell Browser, right-click the drive for which you wish to calculate the throughput, and then click **Show Throughput**.
2. From the Show Drive Throughput dialog box, enter the number of hours for which you wish to view the information.
3. Click **Show.**

   The read and write throughput is displayed in the appropriate boxes.
4. Click **Close** to exit the dialog box.

To view the drive throughput for the past hour

1. In the CommCell Browser, right-click the drive for which you wish to view the throughput, and then click **Properties**.
2. Click the Hardware Info tab.
3. The drive throughput for the past one hour is displayed.

MARK A DRIVE AS CLEANED

Required Capability: Capabilities and Permitted Actions

To mark a drive as cleaned:

1. From the CommCell Browser, right-click the drive that you have cleaned, and then click **Mark Drive Cleaned**.
2. If you are sure that you want to reset the cleaning counters for the drive, click **Yes** in the Confirm prompt that appears.

   The system resets the counters that are linked to the cleaning operation. You can view these counters from the Drive Properties (Odometers) tab.

MARK A DRIVE AS FIXED

*Required Capability***:** Capabilities and Permitted Actions

To mark a drive as fixed:

1. From the CommCell Browser, right-click the drive that you wish to mark as fixed, and then click **Mark Drive Fixed**.
2. Click **Yes** in the Confirm prompt that appears. This will switch the status of the drive as *Online* and reset counters for **Software and Hardware Errors**

(Since Cleanup) for the drive.

You can view the drive counters from the Odometers tab of **Drive Properties**.

Mark a Drive as Replaced

Required Capability: Capabilities and Permitted Actions

▶ To mark a drive as replaced:

1. From the CommCell Browser, right-click the drive that you have replaced, and then click **Mark Drive Replaced**.
2. Click **Yes** in the Confirm prompt that appears.

   This will reset the counters for the drive,

Reset a Drive From the CommCell Console

Required Capability: Capabilities and Permitted Actions

▶ To reset a drive:

1. Be certain that the drive that you want to reset is not in use. Use the Job Controller to find and stop/kill any jobs that use the drive.
2. From the CommCell Browser, right-click the drive that you want to reset, and then click **Reset Drive**.
3. A Confirm Reset prompt appears, informing you that this procedure will unmount any media that are mounted, an operation which may take some time. If you are sure that you want to reset the drive, click **Yes**.

   If the drive is active, an error message will be displayed.

Unload a Drive

Required Capability: Capabilities and Permitted Actions

▶ To unload a drive:

1. Make sure that no jobs are running to the drive that you want to unload, and that the drive contains media.
2. From the CommCell Browser, right-click the drive that you want to unload, and then click **Unload Drive**.
3. If you are sure that you want to unload the drive, click **Yes** in the Confirm prompt that appears.

   If the drive is active, an error message will be displayed.

Validate Drives

▶ To validate a drive

1. From the CommCell Browser, right-click the drive that you wish to validate, and then click **Validate Drive**.
2. From the Validate Drive dialog box, select the necessary options.
3. Click **OK**.

   You can track the progress of the operation in the Event Viewer.

Change the Drive Name

▶ To change the library name:

1. Display the Library and Drive Configuration window.
2. Right-click the drive for which you wish to change the name, and then click **Properties**.
3. In the **Alias** box, type the new name for the drive.
4. Click **OK** to save the changes.

Drive Cleaning

Topics | How To | Related Topics

OVERVIEW

You must clean each drive periodically or when necessary to remove the oxides that accumulate on the read-write heads. The drive cleaning operation includes the task of mounting the cleaning media into the drive, cleaning the read-write head and unmounting the cleaning media. (The cleaning media will be unmounted after the amount of time specified in the **Cleaning Duration** option available in the Drive Cleaning Threshold Parameters tab of **Hardware Maintenance Thresholds** dialog box.)

> Refer to the drive manufacturer's documentation for the recommended drive cleaning criteria and cleaning duration for each drive type.

Drive cleaning operation must be performed in the following situations:

- When a drive reports that it requires cleaning.
- When the drive cleaning threshold parameters established in the Drive Cleaning Threshold Parameters for the drive are exceeded.

  In both these situations, the drive can be automatically cleaned by the MediaAgent, if the Enable Auto-Cleaning options are enabled in the library.

  If the **Enable Auto-Cleaning** options are not enabled in the library, the drive will be marked **Offline** with the appropriate **Offline Reason**. (This information can be viewed from the Status tab of the **Drive Properties** dialog box.)

The MediaAgent offers several options to both monitor and perform the drive cleaning operation. This includes the following:

- Facility to establish drive cleaning thresholds and cleaning duration. For a detailed description of this feature, see Drive Cleaning Threshold Parameters.
- The **Enable Auto-Cleaning** options, which will automatically clean the drive when the hardware (drive) indicates that it requires cleaning or if the drive cleaning threshold parameters are exceeded. For a detailed description of this feature, see Enable Automatic Drive Cleaning.
- The **Clean Drive** option, which when initiated, will mount the cleaning media and clean the drive. For a detailed description of this feature, see Manually Initiating a Drive Cleaning Operation using the CommCell Console.
- Manually clean the drive, without using any of the options available in the CommCell Console. In this case you must mark the drive as cleaned from the CommCell Console after the drive cleaning operation completes successfully. For more information, see Resetting Counters When Drives are Cleaned using Library Options.

  > Some libraries and drives do not support the drive cleaning feature. Refer to the manufacturer's documentation for information on whether the library supports the cleaning feature.

- Schedule the drive cleaning operation so that the drives are cleaned regularly at fixed intervals. See Scheduling Drive Cleaning Operations for more information.

In addition, the system provides the facility to automatically identify the barcodes associated with cleaning media. See Automatically Identify the Cleaning Media using Barcodes.

The **Bull Calypso Media & Library Manager** service on the CommServe checks for drives (in the CommCell) that require cleaning, every 20 minutes. You can modify the frequency by changing the **Automatic Drive Cleaning check interval in Minutes** default value in the Media Management Configuration (Service Configuration) dialog box.

ENABLE AUTOMATIC DRIVE CLEANING

The MediaAgent automatically mounts the cleaning tape and cleans the drive if the **Enable Auto-Cleaning** options are enabled for the library These options are not enabled by default.

If you enable this option, verify and ensure that you have a good cleaning media in the Cleaning Media pool. (For information on the Cleaning Media pool, see

Cleaning Media.)

When a drive is successfully cleaned, a message is displayed in the **Event Viewer**, and the drive cleaning parameters in the Odometers tab of **Drive Properties** are reset.

Keep in mind that if these options are not enabled, the system does not automatically clean the drive when the hardware indicates that the drive requires cleaning. Hence subsequent mount operations in the drive may fail.

This option is not available for stand-alone drives and optical libraries.

> Some drives do not support the drive cleaning feature. Do not enable the Enable Auto-Cleaning option for such drives.

The Enable Auto-Cleaning options can be established from the **General** tab of the **Library Properties** dialog box. The following options can be established:

- On sense code

  Whenever the hardware indicates that a drive requires cleaning, the MediaAgent will automatically mount the cleaning media and clean the drive if you enable the On Sense Code option.

  By default the **On Sense Code** option is disabled for a library. .
- When thresholds exceed

  When a drive exceeds the threshold values established for the drive type in the **Drive Cleaning** tab of **Hardware Maintenance Thresholds** dialog box, the system will automatically mount the cleaning media and clean the drive if you enable the **When Thresholds Exceed** option.

  By default the **When Thresholds Exceed** option is disabled for a library.
- Wait n day(s) after last cleaning

  If you do not want to frequently clean the drives, you can specify the number of days that the MediaAgent must wait after performing an automatic drive cleaning operation, by enabling the **Wait n day(s) after last cleaning** option and specifying the number of days.

  By default this option gets enabled when you select the **On sense code** or **When thresholds exceed** options. The default number of days to wait is set to 3.
- Continue using drive even if it needs cleaning during restore

  If you would like to use a drive even if it requires to be cleaned (Indicated as requires cleaning by either the **On sense code** or **When thresholds exceed** options) enable the **Continue using drive even if it needs cleaning during restore** option.

  This option is not enabled by default.

By default, the MediaAgent checks for drives that require cleaning every 15 minutes. You can modify this value using the **Automatic Drive Cleaning check interval in Minutes** option from the Media Management Configuration (Service Configuration) dialog box available in the **Control Panel**.

SCHEDULING DRIVE CLEANING OPERATIONS

Drive cleaning operation can be scheduled to ensure that the drives are cleaned regularly at periodic intervals. Schedules can be created for multiple drives from the library level in the CommCell Browser. In addition, schedules can also be created for the individual drives at the drive level. When the schedule is executed the job will be displayed in the Event Viewer. After the successful completion of the cleaning operation, the system resets the counters that are linked to drive cleaning. You can view these counters from the Drive Properties (Odometers) tab.

The scheduled drive cleaning operation is not available for stand-alone drives and Optical libraries.

MANUALLY INITIATING A DRIVE CLEANING OPERATION USING THE COMMCELL CONSOLE

Use the **Clean Drive** option available in the CommCell Console for each drive, to manually initiate a drive cleaning operation. When initiated, the **Clean Drive** operation, mounts the cleaning tape and cleans the drive. in addition, this operation also resets the counters that keep track of the number of drive events that have occurred since the drive was cleaned. (These counters can be viewed in the Odometers tab of **Drive Properties**.) The drive cleaning operation can also be scheduled if necessary.

Check the following before starting the drive cleaning operation:

- Ensure that you have imported or moved cleaning media into the Cleaning Media Pool. For more information on importing cleaning media, see Import Cleaning Media.
- If a job is in progress in the drive you wish to clean, the drive cleaning operation would fail. Ensure that the drive is free, before you start the operation.
- In order to perform the **Clean Drive** operation from the CommCell Console, the library's auto-cleaning feature must be disabled from the library's front panel menu.

  Refer to the library manufacturer's documentation for information on disabling the library's auto-clean option from the library's front panel.

The drive cleaning operation is not available for stand-alone drives and Optical libraries.

RESETTING COUNTERS WHEN DRIVES ARE CLEANED USING LIBRARY OPTIONS

Some libraries provide menu options in the library front panel to clean drives. If you use these options, you must indicate to the MediaAgent that the drive has been cleaned.

This can be done by using the **Mark Drive Cleaned** option in the CommCell Console. This will reset the following counters that keep track of the number of drive events that have occurred since the drive was cleaned:

- Number of hours used after last clean
- Number of soft errors after last clean
- Number of hard errors after last clean

These counters can be viewed in the Odometers tab of **Drive Properties**.

Whenever you clean stand-alone drives, use this option from the CommCell Console to indicate that the drive has been cleaned.

AUTOMATICALLY IDENTIFY CLEANING MEDIA USING BARCODES

Most cleaning media have a standard barcode pattern. This feature can be used to automatically identify the cleaning media in the library and move them to the cleaning media pool. This is done as follows:

1. Enable the automatic media discovery option in the Media tab of the **Library Properties** dialog box.
2. Define all the barcode patterns that may be used in all libraries in the CommCell from the **Barcode Patterns** tab of the **Media Management** dialog box.
3. Associate the barcode patterns for cleaning media used in the library, from the **BarCode Patterns** tab of the **Cleaning Media Group Properties** dialog box.

Back to Top

Drive Cleaning - How To

Topics | How To | Related Topics

Enable (or Disable) Automatic Drive Cleaning

Clean a Drive

Schedule Drive Cleaning

Mark a Drive as Cleaned

Modify Drive Cleaning Threshold Parameters

Enable (or Disable) the Checking for Cleaning Media Loaded in the Drive

Add/Modify Bar Code Patterns for Cleaning Media in a CommCell

Associate (or Disassociate) Bar Code Patterns to a Media Group

ENABLE (OR DISABLE) AUTOMATIC DRIVE CLEANING

Required Capability: Capabilities and Permitted Actions

To enable or Disable automatic drive cleaning:

1. From the CommCell Browser, right-click the library for which you wish to enable the automatic drive clean options, and then click **Properties**.
2. Click the Drive tab.
3. Select the necessary options in the **Enable Auto-Cleaning** area.
4. Click **OK** to save the changes.

CLEAN A DRIVE

Before you Begin

- Do not clean the drive when a job is in progress.
- Ensure that you have imported or moved cleaning media into the Cleaning Media Pool. For more information on importing cleaning media, see Import Cleaning Media.
- If a job is in progress in the drive you wish to clean, the drive cleaning operation would fail. Ensure that the drive is free, before you start the operation.
- For the MediaAgent to perform the Clean Drive function, the library's auto-cleaning feature must be disabled from the library's front panel menu.

  Refer to the library manufacturer's documentation for information on disabling the library’s auto-clean option from the library’s front panel.

To clean a drive

To clean multiple drives in the library:

1. From the CommCell Browser, right-click the library in which you wish to clean the drives, and then click **Clean Drive**.
2. From the Clean Drive window, click the drives that you wish to clean. (Use CTRL + click to select multiple drives.)
3. Click **OK**.

   You can track the progress of the operation in the Event Viewer.

To clean a specific drive in the library:

1. From the CommCell Browser, right-click the drive you wish to clean, and then click **Clean Drive**.
2. From the Clean Drive window, click **OK.**

   You can track the progress of the operation in the Event Viewer.

NOTES

After the successful completion of the cleaning operation, the counters linked to drive cleaning are reset. You can view these counters from the Drive Properties (Odometers) tab.

SCHEDULE DRIVE CLEANING

Before you Begin

- Ensure that you have a cleaning media available in the Cleaning Media Pool.
- If a job is in progress in the drive you wish to clean, the drive cleaning operation would fail. Hence, ensure that the drive cleaning operation is scheduled when no other jobs are scheduled or initiated.
- For the MediaAgent to perform the Clean Drive function, the library's auto-cleaning feature must be disabled from the library's front panel menu.

  Refer to the library manufacturer's documentation for information on disabling the library’s auto-clean option from the library’s front panel.

To schedule the drive cleaning operation:

To create schedules for multiple drives in the library:

1. From the CommCell Browser, right-click the library to which the drives are attached, and then click **Clean Drive**.
2. From the Clean Drives dialog box, click the drives for which you wish to create the schedules. (Use CTRL + click to select multiple drives.)
3. Click **Schedule**.
4. From the Schedule Details (Schedule Details) dialog box, create the necessary schedule for this operation.
5. Click **OK** to save the schedule.

   The drive cleaning operation will be executed according to the specified schedule.

To create schedules for a specific drive in the library:

1. From the CommCell Browser, right-click the drive for which you wish to create schedules, and then click **Clean Drive**.
2. From the Clean Drive dialog box, click the **Schedule** option and then click **OK.**
3. From the Schedule Details (Schedule Details) dialog box, create the necessary schedule for this operation.
4. Click **OK** to save the schedule.

   The drive cleaning operation will be executed according to the specified schedule.

NOTES

After the successful completion of the cleaning operation, the MediaAgent resets the counters that are linked to drive cleaning. You can view these counters from the Drive Properties (Odometers) tab.

MARK A DRIVE AS CLEANED

Required Capability: Capabilities and Permitted Actions

To mark a drive as cleaned:

1. From the CommCell Browser, right-click the drive that you have cleaned, and then click **Mark Drive Cleaned**.
2. If you are sure that you want to reset the cleaning counters for the drive, click **Yes** in the Confirm prompt that appears.

   The system resets the counters that are linked to the cleaning operation. You can view these counters from the Drive Properties (Odometers) tab.

MODIFY DRIVE CLEANING THRESHOLD PARAMETERS

Required Capability: See Capabilities and Permitted Actions

To modify drive cleaning threshold parameters:

1. From the **Tools** menu in the CommCell Console, click **Control Panel.**
2. Double-click **Hardware Maintenance**.
3. Click the Drive Cleaning tab.
4. Click the drive type for which you wish to modify the thresholds, and then click **Edit**.
5. In the Drive Cleaning Threshold Parameters dialog box, modify the necessary threshold values, and then click **OK**.
6. Click **OK** in the **Hardware Maintenance Thresholds** dialog box to save the changes.

ENABLE (OR DISABLE) THE CHECKING FOR CLEANING MEDIA LOADED IN THE DRIVE

Required Capability: Capabilities and Permitted Actions

To enable or disable the checking for cleaning media loaded in the drive:

1. From the CommCell Browser, right-click the library for which you wish to enable or disable this option, and then click **Properties**.
2. Click the Drive tab.
3. From the **Attributes** region, choose **Check for cleaning media loaded in Drive** to enable this option. (Clear this check box to disable this option.)
4. Click **OK** to save the changes.

ADD/MODIFY BARCODE PATTERNS FOR MEDIA IN A COMMCELL

Required Capability: See Capabilities and Permitted Actions

To add/modify barcode patterns for media in a CommCell:

1. From the **Tools** menu in the CommCell Console, click **Control Panel.**
2. Double-click **Media Management Configuration**.
3. Click the BarCode Patterns tab.
4. Click **Add**.

   or

   Click the pattern and then click **Edit** to modify an existing pattern.
5. From the BarCode Pattern dialog box establish a barcode pattern using the various options provided.
6. Click **OK**. The pattern is displayed in the **Add / Edit / Remove Pattern** box.
7. Click **OK** to save the changes.

Associate (or Disassociate) Barcode Patterns to a Media Group

Required Capability: See Capabilities and Permitted Actions

➧ To associate (or disassociate) barcode patterns to a Media Group:

1. From the CommCell Browser, right-click the appropriate media group (**Default** or ***<user-defined>* scratch pools**, **Cleaning Media**, or **Foreign Media** group) and then click **Properties**.
2. Click the Barcode Patterns tab.
3. To associate a barcode, click the barcode you wish to associate from the **Available Patterns** list and then click **Add**.

   If the **Available Patterns** list does not contain the specific barcode pattern used in the library, add the pattern as described in Add Barcode Patterns for Media in a CommCell.
4. To disassociate a barcode, click the barcode you wish to disassociate from the **Selected Patterns** list and then click **Remove**.
5. Click **OK** to save the changes.

The selected barcodes will be used to identify media and automatically move them to the appropriate Media pool, if the **Enable Auto-Discover Media into default scratch pool** option is enabled in the Library Properties (Media) tab.

Pre-Post Drive Commands

Topics | How To | Related Topics

This tool provides the ability to run customized scripts to gather information before or after drive load and unload phases from the command line.

The pre-post drive commands are supported for the Unix and Windows MediaAgents. These commands are not supported for NetWare MediaAgents.

Pre-Post Drive Commands - How To

Topics | How To | Related Topics

SET-UP PRE-POST DRIVE COMMANDS

The pre-post drive commands can be setup by running an executable from the command prompt, available in the following locations:

- Windows: `<`*`Software Installation Path`*`>\Base\AddPrePostCmdForDrives.exe`
- Unix: `<`*`Software Installation Path`*`>/Base/AddPrePostCmdForDrives.exe`

This is menu driven program and can be used both to add or remove a pre-post drive command. This program will prompt you for the following information:

1. The name of the library.
2. Whether the command must be run on a specific drive or all drives.
3. The phase in which the command must be run. Available phases are `preload`, `postload`, `preunload` or `postunload`.
4. If you had previously added a command, whether you wish to add or remove a command.
5. The path to the script or executable that must run.
6. Any additional argument that may be required to run the script or executable. The following arguments can be added to the script or executable:

   %DriveName

   %LibraryName

   %DriveAccessPath

   %DriveSerialNo

   %MediaAgent

   %JobID
7. For Windows, the user impersonation details that must be used to execute the script or executable, such as the user name, password and/or domain name. User impersonation is not applicable for Unix.

The command will be saved in the following location and will be automatically executed during the specified phase of the drive load/unload operations:

- Windows: `<`*`Software Installation Path`*`>\MediaAgent\PrePostDriveCmd.txt`
- Unix: `<`*`Software Installation Path`*`>/MediaAgent/PrePostDriveCmd.txt`

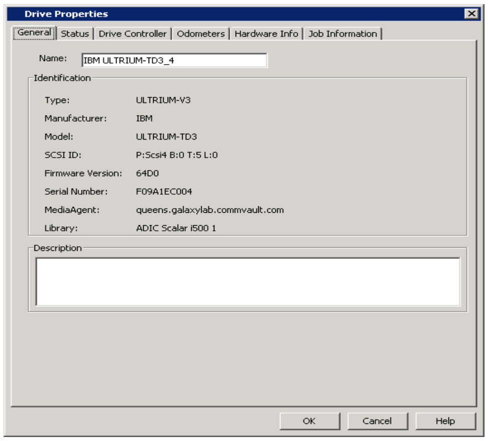
Drive Properties

Topics | How To | Related Topics

GENERAL

The general information about the drive, including the drive type, manufacturer, SCSI ID and firmware version, MediaAgent and library controlling the drive and a list of compatible media formats that can be used in the drive are displayed.

If necessary you can use the description field to record additional information about the Drive.



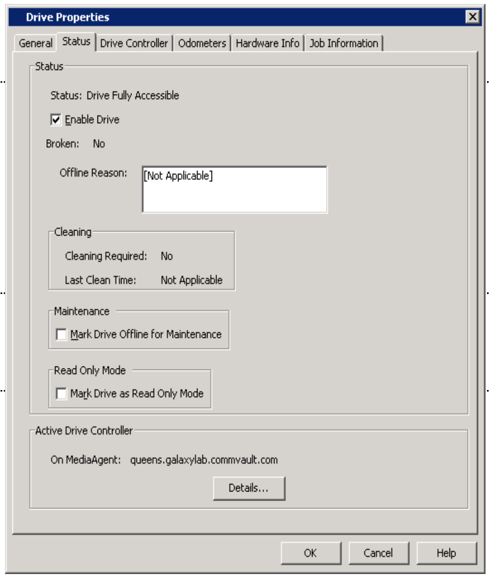
Name: IBM ULTRIUM-TD3_4

Identification

Type: ULTRIUM-V3
Manufacturer: IBM
Model: ULTRIUM-TD3
SCSI ID: P:Scsi4 B:0 T:5 L:0
Firmware Version: 64D0
Serial Number: F09A1EC004
MediaAgent: queens.galaxylab.commvault.com
Library: ADIC Scalar i500 1

Description

STATUS



Status

Status: Drive Fully Accessible
☑ Enable Drive
Broken: No
Offline Reason: [Not Applicable]

Cleaning

Cleaning Required: No
Last Clean Time: Not Applicable

Maintenance

☐ Mark Drive Offline for Maintenance

Read Only Mode

☐ Mark Drive as Read Only Mode

Active Drive Controller

On MediaAgent: queens.galaxylab.commvault.com

- ### STATUS

  You can view the current status of the drive, including the drive online/offline, broken and cleaning status.

  You can use the **Enable Drive** option to logically enable or disable the drive in the CommCell.

  The drive status is displayed as **Offline** in situations in which a job cannot access the drive. In addition the **Offline Reason** drive indicates the appropriate reason.

- ### CLEANING

  You can view information on whether the drive requires cleaning and the last clean time, if applicable.

- ### MAINTENANCE

  Mark Drive Offline for Maintenance

  You can enable this option when you wish to perform routine or other maintenance tasks on devices. This option is available in the MediaAgent, Library and Drive levels and you can appropriately enable them where needed.

  Data protection, data recovery and auxiliary copy operations will not use the associated MediaAgent/Library/Drive, depending on where the option is enabled. However, other administrative tasks on the devices such as Full Scan, Drive Cleaning, Verify Media etc. can be performed, if required.

  When this option is enabled, the system will automatically select an alternate resource (MediaAgent/Library/Drive) if Alternate Data Paths (GridStor) is enabled. If alternate resources are not available, data protection, data recovery and auxiliary copy will remain in the `Waiting` state in the **Job Controller** and will automatically resume when you re-enable the appropriate MediaAgent/Library/Drive.

- **READ ONLY MODE**

  Mark Drive as Read Only Mode

  You can enable this option when you wish to exclusively reserve a drive for data recovery operations. When this option is enabled the system will automatically select an alternate drive for write operations. If an alternate drive is not available the write operations (e.g., data protection, auxiliary copy, etc.) will remain in the `Waiting` state in the **Job Controller** and will automatically resume when you re-enable the appropriate drives.

  > When **Mark Drive Offline for Maintenance** and/or **Mark Drive as Read Only Mode** options are enabled, if a media is already mounted in the drive, the drive may continue to be used until the media is unmounted.

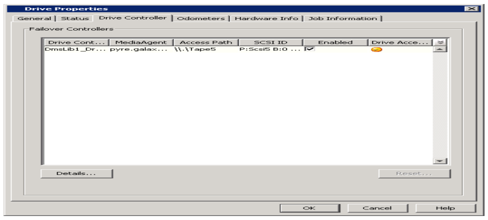
- **ACTIVE DRIVE CONTROLLER**

  This option is useful to determine whether the drive controller in a specific MediaAgent is active or not.

DRIVE CONTROLLER

The **Drive Controller** tab is useful to determine whether the drive controller in a specific MediaAgent is active or not.

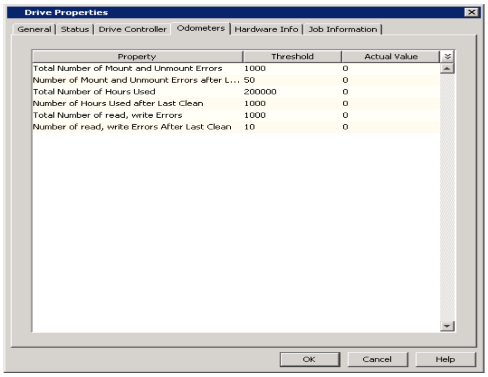
In a SAN environment, where multiple MediaAgents share the drives in a library using Dynamic Drive Sharing (DDS), the information in the drive controller tab can be used to identify all the MediaAgents that share a drive. If necessary the drive controller from a specific MediaAgent can be marked as disabled, if there is a problem using the drive from a specific MediaAgent.



Drive Cont...	MediaAgent	Access Path	SCSI ID	Enabled	Drive Acce...
DmsLib1_Dr...	pyre.galax...	\\.\Tape5	P:Scsi5 B:0 ...	☑	●

ODOMETERS

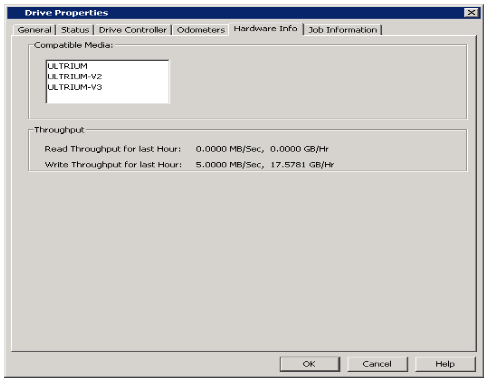
To ensure that drives are cleaned and replaced when necessary, the system keeps track of various types of drive events. For each drive, the system tracks the number of times each event occurs. When the number of events exceeds the preset maintenance threshold, e status of the drive is displayed as **Offline** and a suitable message is displayed in the **Event Viewer**, notifying you that the drive requires cleaning or replacement. In addition, the **Threshold Exceeded Alert** is generated, if configured. For information on setting the drive maintenance parameters, see Drive Maintenance Threshold Parameters.



Property	Threshold	Actual Value
Total Number of Mount and Unmount Errors	1000	0
Number of Mount and Unmount Errors after L...	50	0
Total Number of Hours Used	200000	0
Number of Hours Used after Last Clean	1000	0
Total Number of read, write Errors	1000	0
Number of read, write Errors After Last Clean	10	0

HARDWARE INFO

The hardware information tab displays the compatible media types that can be used on the drive and the drive throughput information.



Compatible Media:

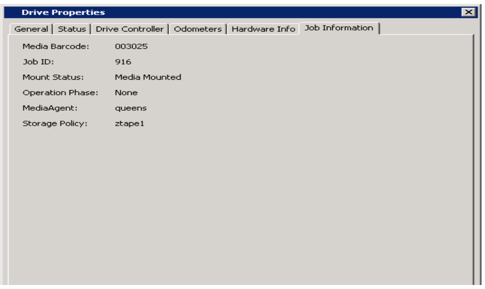
ULTRIUM
ULTRIUM-V2
ULTRIUM-V3

Throughput

Read Throughput for last Hour: 0.0000 MB/Sec, 0.0000 GB/Hr
Write Throughput for last Hour: 5.0000 MB/Sec, 17.5781 GB/Hr

JOB INFORMATION

The Job Information tab is displayed in the **Drive Properties** dialog box when a job is active in the drive. The job information provides details and status information associated with the operation in the drive.



Media Barcode: 003025
Job ID: 916
Mount Status: Media Mounted
Operation Phase: None
MediaAgent: queens
Storage Policy: ztape1

Drive Properties - How To

Topics | How To | Related Topics

Mark MediaAgent/Library/Drive Offline for Maintenance

Required Capability: Capabilities and Permitted Actions

To mark MediaAgent/Library/Drive Offline for Maintenance:

1. From the CommCell Browser, right-click the MediaAgent/Library/ Drive that you wish to mark offline for maintenance, and then click **Properties**.
2. Select one or more of the following options as appropriate:
   - To mark a MediaAgent offline for maintenance: Click the Control tab and then click and enable the **Mark MediaAgent Offline for Maintenance** option.
   - To mark a library offline for maintenance: Click the Status tab and then click and enable the **Mark Library Offline for Maintenance** option.
   - To mark a drive offline for maintenance: Click the Status tab and then click and enable the **Mark Drive Offline for Maintenance** option.
3. Click **OK** to save the configuration.

   Subsequent data protection, data recovery and auxiliary copy operations will not use the associated MediaAgent/Library/Drive.

Mark a Drive for Read-Only Operations

Required Capability: Capabilities and Permitted Actions

To mark a drive for read-only operations:

1. From the CommCell Browser, right-click the drive that you wish to mark as read-only, and then click **Properties**.
2. Click the Status tab.
3. Click **Mark Drive as Read Only Mode** to enable the option.
4. Click **OK** to save the information.

View the Drive Offline Reason

Required Capability: Capabilities and Permitted Actions

To view the offline reason for a drive:

1. From the CommCell Browser, right-click the drive for which you wish to view the offline reason, and then click **Properties**.
2. Click the Status tab.

   Information on the drive offline reason is displayed in the **Offline Reason** box.

VIEW THE STATUS OF THE DRIVE CONTROLLER

Required Capability: Capabilities and Permitted Actions

To view the status of the drive controller:

1. From the CommCell Browser, right-click the drive for which you wish to view the drive controller status, and then click **Properties**.
2. Click the Drive Controller tab.

   The status of the drive controller can be viewed in the **Drive Properties (Drive Controller)** dialog box. Note the following:

   The **Active Library Controller** is the MediaAgent with the **Active**, **Alive** and **Enabled** status as YES, and the **Soft State** as *ON*. (You can view the status of the library controllers by clicking the **Detail** button on the **Active Library Controller** or **Failover Library Controller** panes.)

   - In a library configured in the SAN environment, where several MediaAgents are configured as library controllers, at any given point, the MediaAgent accessing the library is considered as **Active** and therefore displayed as the Active Library Controller. All the other MediaAgents are displayed as **Failover Library Controllers**. The **Active** status will be displayed as *No* for the failover library controllers.
   - In a library configured in the non-SAN environment, where only one MediaAgent is configured as a library controller, the MediaAgent is displayed as the Active Library Controller. If either the Alive or Enabled status is NO, or Soft State is OFF, the Active status will be displayed as OFF and the MediaAgent will be displayed as a **Failover Library Controller**.

VIEW THE DRIVE USAGE INFORMATION

To view the drive usage information:

1. From the CommCell Browser, right-click the drive for which you wish to view the usage information, and then click **Properties**.
2. Click the Odometer tab.

   The usage information is displayed.

VIEW THE DRIVE THROUGHPUT

To calculate the drive throughput for a specified time

1. In the CommCell Browser, right-click the drive for which you wish to calculate the throughput, and then click **Show Throughput**.
2. From the Show Drive Throughput dialog box, enter the number of hours for which you wish to view the information.
3. Click **Show.**

   The read and write throughput is displayed in the appropriate boxes.
4. Click **Close** to exit the dialog box.

To view the drive throughput for the past hour

1. In the CommCell Browser, right-click the drive for which you wish to view the throughput, and then click **Properties**.
2. Click the Hardware Info tab.
3. The drive throughput for the past one hour is displayed.

ENABLE (OR DISABLE) A DRIVE

Required Capability: Capabilities and Permitted Actions

To enable or disable a drive:

1. From the CommCell Browser, right-click the drive you wish to enable or disable, and then click **Properties**.
2. Click the Status tab.
3. In the **Status** area, click **Enable Drive**.
4. Click **OK** to save the changes.

ENABLE (OR DISABLE) A DRIVE FROM A SPECIFIC MEDIAAGENT

Required Capability: Capabilities and Permitted Actions

▶ To enable or disable a drive from a specific MediaAgent:

1. From the CommCell Browser, right-click the drive you wish to enable or disable, and then click **Properties**.
2. Click the Drive Properties (Drive Controller) tab.
3. In the **Failover Controllers** area, click the **Enabled** option for the specific MediaAgent.

   To enable or disable multiple drives, select all the drives you wish to enable or disable, right-click, and then select **Enable** (or **Disable).**
4. Click **OK** to save the changes.

CHANGE THE DRIVE NAME

▶ To change the library name:

1. Display the Library and Drive Configuration window.
2. Right-click the drive for which you wish to change the name, and then click **Properties**.
3. In the **Alias** box, type the new name for the drive.
4. Click **OK** to save the changes.

VIEW THE JOB INFORMATION

▶ To view the job information:

1. In the CommCell Browser, right-click the drive for which you wish to view the job information, and then click **Properties**.

   Note that a job should currently be running in the drive to view the job information associated with the job.
2. Click the **Job Information** tab.
3. Click **OK** to exit the dialog box.

DECONFIGURE DRIVES

Before you Begin

The number of configured drives in a drive pool cannot be smaller than the largest number of streams used by any storage policy that accesses that drive pool. For example, assume that a drive pool containing four drives is accessed only by a three-stream storage policy. In this case, you can deconfigure only one drive within the drive pool. The system prevents you from deconfiguring any additional drives. To deconfigure additional drives, you must first reduce the number of streams in the storage policy.

> Some Agents/database applications have the following requirement: The number of streams through which the database is restored must equal the number of streams through which the data was backed up. If you have used a storage policy for multi-stream database backups we advise you not to reduce the number of streams.

▶ To deconfigure a drive:

1. Be certain that the drive that you want to deconfigure is not in use. Use the Job Controller to find and kill any jobs that use the drive. (For information on the killing a job from the Job Controller see Killing a Job.)
2. Make sure that a media is not mounted in the drive.
3. Display the Library and Drive Configuration window.
4. Right-click the drive that you want to deconfigure, and then click **Deconfigure**.
5. Click **Yes** in the confirmation prompt that appears to deconfigure the drive.

   The status of the drive changes to **not configured**.

Media Operations

Topics | How To | Troubleshoot | Related Topics

OVERVIEW

The following sections describe the various media related operations that can be performed in a tape/optical library.

The media options vary depending on how the library is configured. The following table provides a list of the media operations in the blind/sighted libraries and stand-alone drives.

OPTIONS	**REGULAR LIBRARY (WITH A BARCODE READER)**	**BLIND LIBRARY (WITHOUT A BARCODE READER)**	**STAND-ALONE DRIVE, AND REMOVABLE DISK DISK STORAGE**	**PNP (PLUG AND PLAY) DISK LIBRARIES**
Load Media	**X**	**X**		
Export	**X**	**X**		
Verify Media	**X**	**X**	**X**	**X**
View Contents	**X**	**X**	**X**	**X**
Move	**X**	**X**		
Delete	**X**	**X**	**X**	**X**
Delete Contents	**X**	**X**	**X**	**X**
Erase Media	**X**	**X**		
Discover	**X**	**X**		
Mark Media Bad	**X**	**X**	**X**	**X**

Mark Media Good	X	X	X	X
Mark Media Full	X	X	X	X
Mark Appendable	X	X	X	X
Mark Media Reusable	X	X	X	
Stamp Media			X	
Erase Media	X	X	X	

MEDIA BLOCK SIZES

MediaAgents can write to media using different block sizes, if the Operating System associated with the MediaAgent in which the library is configured supports a higher block size. The system can write block sizes up to 256 KB and can automatically read block sizes up to 512 KB. If the block sizes are larger than 512 KB, read operations from the media will fail. Also note that such media will be over written and re-used if the **When Content Verification Failed** option is enabled in the **Library Properties (Media)** dialog box

Block sizes can be modified from the **Data Path Properties** dialog box available from the **Data Paths** tab of the **Copy Properties** dialog box, for the specific data path. (See Set the Chunk Size and Block Size for a Data Path for step-by-step instructions.)

See Also: Performance Tunables for Media Management

AUDIT TRAIL

Operations performed with this feature are recorded in the Audit Trail. See Audit Trail for more information.

LOAD MEDIA

The load media operation loads the media into the drive. You can initiate the load media by right-clicking the media that you wish to load and then choosing the **Load Media** option.

See Load a Media to a Drive for step-by-step instructions.

UNLOAD MEDIA

You can select the media from the drive and unload it if necessary.

EXPORT MEDIA

Media residing within a library can be exported to physically remove it from the library. For comprehensive information on exporting media, see Export Media.

RECALL MEDIA

The Recall Media feature provides the facility to temporarily bring media back from an export location for a specific operation and return the media to the export location when the operation is complete. For comprehensive information on this option, see Recall Media.

See Recall Media using the Resource View for step-by-step instructions.

VERIFY MEDIA

The verify media operation is a type of inventory which must be initiated by the user. This operation can be used to verify whether the media information displayed in the CommCell Console matches the OML in the media. You can initiate the verify inventory operation by right-clicking the media that you wish to verify and then choosing the **Verify Media** option.

A verify inventory operation is displayed as a job in the **Job Controller** window and can be **killed** if necessary.

The verify inventory operation does not discover new media.

See also, Verify Media for Blind Libraries.

VIEW CONTENTS

You can view the contents of a specific used media. This feature can be used to view a list of data protection operations residing in the media, including the data protection operations currently in progress. All the details associated with the data protection operation(s) available in the media are displayed. This includes the following:

- The Job ID associated with the data protection operation

- Names of the client, agent, instance/backup set and subclient
- Whether the data protection operation is Full, Incremental, Differential or Synthetic full
- The archive file type
- The day and time in which the archive file associated with the data protection operation was created
- Media side
- Archive file
- See View the Contents of a Media for step-by-step instructions.

MOVE MEDIA

You can move spare media between the following pools:

- Scratch pools
- Cleaning Media pools
- Overwrite Protect Media pools
- Foreign Media pools

The facility to logically reassign media from one scratch pool to another allows you to ensure that critical operations always have the media that they need. You can also select multiple media and move them from one scratch pool to another.

See the following procedures for step-by-step instructions:

- Move a Media From One Scratch Pool to Another
- Move Media in Bulk From One Scratch Pool to Another

MOVE MEDIA TO LIBRARY

You can move the following Media to Libraray:

- Orphaned Media - The Orphaned media does not have any associated library. You can move an orphaned media to a library. For step-by-step instructions, see Move Orphaned Media to Library.
- Exported Media - The Exported media is the media which were previously discovered and subsequently exported from the library. You can move the exported media to a library. For step-by-step instructions, see Move Export Media to Library.

DELETE MEDIA

The delete media option can be used to delete the media information from the CommCell. Spare and retired media can be deleted to remove them from the scratch pool and Retired Media group. When a media is deleted, the media information is permanently removed from the CommServe database. You can also select multiple media from the scratch pool, and delete them if necessary.

See Delete a Media for step-by-step instructions.

DELETE CONTENTS

The delete contents option can be used to delete the contents of a media and move it to a specified scratch pool. This option can be used to make media available to complete an important data protection job when there are no spare media available in the library.

> **Caution**
>
> Once deleted, the contents of the media are not available for data recovery operations, and the system will not automatically force the next data protection operation to be a full backup. If you delete the contents of the media, you should immediately run a full backup for all the subclients associated with the media once the operations is complete.

If you have a library configured with mixed drive types, verify and ensure that the media is moved to a drive pool associated with the specific media type.

See Delete the Contents of a Media for step-by-step instructions.

If you have the need to recover data from a media in which the contents has been deleted, see Accessing Aged Data.

PREVENT COPY

Prevent Copy option allows you to disable all the existing jobs in the specified media from being copied.

ALLOW COPY

Allow Copy option allows you to enable the (previously disabled) copy jobs from the specified media.

RE-COPY

Re-Copy option allows you to select the existing jobs in the specified media for re-copy. When the re-copy option is selected, the existing jobs will be deleted and selected for re-copy. If the source copy is not available for a job, the existing copy will be retained as is. Re-Copy can be done only on media associated with a secondary copy.

DISCOVER MEDIA

The discover media operation is specific to blind libraries. For comprehensive information on this option, see Discovering Media for Blind Libraries.

MARK MEDIA BAD

If you know that an existing spare or used media is bad, you can mark the media as bad. This will automatically moves the spare media to the **Retired Media** pool. Note however, if the media is a used or **Assigned** media, the media will be moved to the **Retired Media** pool only when the data available in the media is pruned.

See Mark a Media Bad for step-by-step instructions.

MARK MEDIA GOOD

If you know that a bad media in the **Retired Media** pool is fixed and currently usable, you mark the media as good. This will automatically move the media to the **Default Scratch** pool.

See Mark a Bad Media Good for step-by-step instructions.

MARK MEDIA FULL

If for some reason you do not want to use a media for future data protection operation, you can mark the active media full.

You can also mark all active media as full for a storage policy copy.

See Mark a Media Full for step-by-step instructions.

MARK APPENDABLE

You can mark full and bad media as appendable. When a media is marked as appendable it can be re-used by the MediaAgent if the **Use Appendable Media** option is enabled in the Media tab of the **Library Properties** dialog box.

See the following procedures for step-by-step instructions:

- Marking a Media as Appendable
- Reuse Media Marked as Appendable

MARK MEDIA REUSABLE

Media migrated from other CommCell can be marked reusable in the current CommCell, even if the media was not marked for reuse during migration. Multiple media can be selected and marked for reuse in a single operation.

See Mark Media Reusable for step-by-step instructions.

PREVENT EXPORT

You can prevent a media from being exported from the library. Subsequently, you can enable the media for export if necessary. All general media operations can be performed on media that are prevented from being exported. For comprehensive information on exporting media, see Export Media.

ERASE SPARE MEDIA

The erase spare media operation ensures that the data from removable media (tapes and optical platters) are not recoverable once the media is recycled. Only spare, retired and recycled media from tape and optical libraries can be erased. For comprehensive information on erasing media, see Erase Spare Media.

REFRESH MEDIA

Media refresh operation enables you to consolidate the data on media and/or to replace an existing old media. Media refresh can be performed on Full media only. For media refresh options at various levels and instructions to perform media refresh, see Media Refresh.

Media Operations - How To

Topics | How To | Troubleshoot | Related Topics

Load Media

- Load a Media to a Drive

Export Media

- Export a Specific Media

View Contents

- View the Contents of a Media

Move Media

- Move a Media From One Scratch Pool to Another
- Move Media in Bulk From One Scratch Pool to Another

Delete Media

- Delete a Media

Delete Contents

- Delete the Contents of a Media

Erase Media

- Erase Spare Media

Discover Media

- Discover Media from the CommCell Console

Mark Media Bad

- Mark a Media Bad

Mark Media Good

- Mark a Bad Media Good

Mark Media Full

- Mark a Media Full

Mark Media Appendable

- Marking a Media as Appendable
- Reuse Media Marked as Appendable

Mark Media Reusable

- Mark Media Reusable

Prevent Reuse

- Prevent an Assigned Media From Being Reused
- Reuse an Assigned Media that was Prevented From Being Reused

LOAD A MEDIA TO A DRIVE

Required Capability: Capabilities and Permitted Actions

➡ To load a media to a drive:

1. In the left pane of the CommCell Browser, click the **Media in Library** node.

   All the media available in the library are displayed in the right-pane.

2. From the right pane of the CommCell Browser, right-click the media that you want to load into a drive, and then click **Load Media**.

   The **Load Media** option will be displayed only for those media that are available in the library.

3. From the Load Media dialog box specify the resources that must be used to load media into a drive.
4. Click **OK**.

   The system will attempt to load the media into the specified drive. A event message is displayed in the **Event Viewer** after the successful completion of the operation.

EXPORT A SPECIFIC MEDIA

Required Capability: Library Management

➡ To export a specific media:

1. From the CommCell Console select the media you wish to export from one of the following pools or dialog boxes:
   - **Media in Library** (discovered and undiscovered media) pool
   - **Scratch pools**
   - **Cleaning Media** pool
   - **Retired Media** pool
   - **Assigned Media** pool
   - **Media List** dialog box which appears when you select the **View Media** option that appears when you right-click a Storage Policy copy.
   - **Media List** dialog box which appears when you select the **Change Data Path** option that appears when you right-click a Storage Policy copy.
   - **Media Used By Job ID** dialog box which appears when you select the **View Media** option from the **Data Protections Job History**, **Backup Job History,** or **Data Migration History** windows.
2. Right-click the media that you want to export, and then click **Export.**
3. In the **Export Media** dialog box, enter an optional description of the location outside the library where the media will be stored.
4. Click **OK.**

   The location field is for display purposes only, to help you keep track of exported media. The MediaAgent has no control over media once they leave the library; it is your responsibility to ensure that exported media are stored in the location entered.

5. An **Export Media** prompt appears, prompting you remove the media. Do one of the following:
   - If you are exporting through a mail slot, click **OK**, wait for the media to be moved to the mail slot, and then remove them from the library.
   - If you are removing media directly, click **OK**, open the library door, remove the media that you want to export, and then close the door.

VIEW THE CONTENTS OF A MEDIA

Required Capability: Capabilities and Permitted Actions

➡ To view the contents of a media

1. From the CommCell Browser, in the Media in Library pool or the Assigned Media pool, right-click the media for which you wish to view the content, and then click **View Contents**.

   or

   From the Media Used By Job ID dialog box right-click the media for which you wish to view the content, and then click **View Contents**.

2. Click **Yes** in the prompt which displays that the operation may take a few minutes.
3. The Contents of Media dialog box displays the details of jobs available in the media.

Move a Media From One Scratch Pool to Another

Required Capability: See Capabilities and Permitted Actions

To move a media from one scratch pool to another:

1. In the left pane of the CommCell Browser, select the scratch pool containing the media that you want to move. The contents of the scratch pool are displayed in the right pane of the Browser.
2. From the right pane of the CommCell Browser, right-click the media that you want to move, and then click **Move**.
3. In the Move Media dialog box, select the scratch pool to which you want to move the media. If it is cleaning media, select Cleaning Media pool.
4. Click **OK** to complete the transfer.

   The selected media is reassigned to the destination scratch pool.

Move Media in Bulk From One Scratch Pool to Another

Required Capability: See Capabilities and Permitted Actions

To move a number of unspecified media from one scratch pool to another:

1. From the CommCell Browser, right-click the scratch pool from which you want to move media (i.e., the source pool), and then click **Move Media** from the short-cut menu.
2. In the Move Media dialog box, enter the number of media to be moved in the **No. of Media to be moved** field. Select the scratch pool into which you want to move the media from the **Destination Scratch Pool** list.
3. Click **OK** to complete the transfer.

   The selected media is reassigned to the destination scratch pool.

Delete a Media

Required Capability: Capabilities and Permitted Actions

To delete a media

1. In the CommCell Browser, right-click the media you wish to delete, and then click **Delete** Media.
2. Click **Yes** in the prompt asking you to confirm whether you wish to delete the media.
3. From the Delete Contents and Move Media dialog box, select the scratch pool to which you wish to move the media.
4. Click **OK** to save the information.

   The media information is deleted in the CommServe database and moved to the specified scratch pool.

Delete the Contents of a Media

Required Capability: Capabilities and Permitted Actions

> **Caution**
>
> Once deleted, the contents of the media are not available for data recovery operations, and the system will not automatically force the next data protection operation to be a full backup. If you delete the contents of the media, you should immediately run a full backup for all the subclients associated with the media once the operations is complete.

1. In the left pane of the CommCell Browser, select the **Assigned Media** node.

   All the assigned media are displayed in the right-pane.
2. From the right pane of the CommCell Browser, right-click the desired media and select **Delete Contents**.

   NOTES

   The **Delete Contents** option will be displayed only for those media that are available in the library.
3. Click **Yes** to confim. The Enter Confirmation Text dialog displays.
4. Type "erase and reuse media" in the field, and click **OK**.

5. Select the name of the scratch pool to which the media must be moved, after the contents are deleted.
6. Click **OK**.
7. Click **OK** in the warning prompt to continue with the operation.

   The media information is deleted from the CommServe database and the media is moved to the specified scratch pool.

   The operation is recorded in the Audit Trail.

ERASE SPARE MEDIA

To erase spare media:

1. Mark the media to be erased as described in Mark Spare Media for Media Erase Operation.
2. Run the Erase Spare Media operation. This can be done in one of the following ways:
   - Run the Erase Spare Media operation, immediately from the library level, as described in Run a Erase Spare Media Operation Immediately.
   - Schedule an Erase Spare Media operation from the library level, as described in Schedule an Erase Spare Media Operation.
   - Erase a specific spare or retired media, as described in Erase a Specific Spare or Retired Media.

DISCOVER MEDIA FROM THE COMMCELL CONSOLE

You can use the following procedure to:

- Discover all media within a library
- Discover a partial set of media within a library

Required Capability: Capabilities and Permitted Actions

To discover media within a library:

1. From the CommCell Browser, right-click the library whose media you want to discover, and then click **Discover Media**.
2. If one or more new media are discovered, the system displays the Discover New Media dialog box and prompts you for media information.
3. Select the hardware type of the new media from the **New Media Type** list and the scratch pool to which you want the media assigned from the **Destination Scratch Pool** list.
4. The total number of undiscovered media available in the library is displayed in the **No. of media in Free Media Pool** field. Specify the number of media you would like to discover in the **No. of media to be discovered** field.
5. Click **OK**.

You can also discover the media from the **Library and Drive Configuration** window. See Discover Media from the Library and Drive Configuration Window for more information.

MARK A MEDIA BAD

Required Capability: Capabilities and Permitted Actions

To mark a media as bad:

1. In the CommCell Browser, right-click the media you wish to mark as bad, and then click **Mark Media Bad**.
2. Click **Yes** in the prompt asking you to confirm whether you wish to mark the media bad.

   The media status is changed to bad. (Media status can be viewed in the <*Media ID*> tab of the **Media Properties** dialog box.)

MARK A BAD MEDIA GOOD

Required Capability: Capabilities and Permitted Actions

To mark a bad media as good:

1. In the CommCell Browser, from the **Retired Media** Pool, right-click the bad media you wish to mark as good, and then click **Mark Media Good**.
2. Click **Yes** in the prompt asking you to confirm whether you wish to mark the media good.

   The media status is changed to good and the media is moved to the **Default Scratch** pool. (Media status can be viewed in the <*Media ID*> tab of the

Media Properties dialog box.)

MARK A MEDIA FULL

Required Capability: Capabilities and Permitted Actions

To mark a media as full:

1. In the CommCell Browser, from the Media in Library pool or Assigned Media pool, right-click the active media you wish to mark as full, and then click **Mark Media Full**.

   or

   From the Media Used By Job ID dialog box right-click the media you wish to mark as full, and then click **Mark Media Full**.
2. Click **Yes** in the prompt asking you to confirm whether you wish to mark active media full.

   The media status is changed to full. (Media status can be viewed in the <*Media ID*> tab of the **Media Properties** dialog box.)

MARK A MEDIA AS APPENDABLE

Required Capability: Capabilities and Permitted Actions

To mark a media as appendable:

1. In the CommCell Browser, from the Media in Library pool or Assigned Media pool, right-click the exported media you wish to mark as appendable, and then click **Mark Appendable**

   or

   From the Media Used By Job ID dialog box right-click the media you wish to mark as appendable, and then click **Mark Appendable**.
2. Click **Yes** in the prompt asking you to confirm whether you wish to mark the media as appendable.

   The media status is changed to *Appendable* with the reason stating `User marked appendable`. (Media status can be viewed in the <*Media ID*> tab of the **Media Properties** dialog box.)

REUSE MEDIA MARKED AS APPENDABLE

Required Capability: See Capabilities and Permitted Actions

To reuse media marked as appendable:

1. From the CommCell Browser, right-click the library for which you wish to reuse media marked as appendable, and then click **Properties**.
2. Click the Media tab.
3. Click **Use Appendable Media within n Day (s) of its last write time**.
4. Type the number of days that the media can be used after it was marked as appendable.
5. Click **OK** to save the changes.

MARK MEDIA REUSABLE

Required Capability: Capabilities and Permitted Actions

To mark media reusable:

1. In the CommCell Browser, right-click the migrated media you wish to mark as reusable.

   If you wish to reuse more than one migrated media, select all the migrated media you wish to reuse, and then right-click. Hold the Control key down to select more than one media.
2. Click **Mark Media Reusable**.
3. Click **Yes** in the prompt asking you to confirm whether you wish to mark the media reusable.
4. The media will be marked reusable.

PREVENT AN ASSIGNED MEDIA FROM BEING REUSED

Required Capability: See Capabilities and Permitted Actions

To prevent an assigned media from being reused:

1. In the CommCell Browser, navigate to the Assigned Media Pool. The contents of the Assigned Media pool are displayed in the right pane of the Browser.
2. From the right pane, right-click the media that you want to prevent reuse, and then click **Prevent Reuse**.

   Note that this option will be available only if the media was previously NOT prevented from being reused.
3. In the Overwrite Protect Media Group Selection dialog box, select the specific Overwrite Protect Media pool to which you want to move the media when the media is recycled.
4. Click **OK** to save the information.

REUSE AN ASSIGNED MEDIA THAT WAS PREVENTED FROM BEING REUSED

Required Capability: See Capabilities and Permitted Actions

To Reuse an Assigned Media that was Prevented From Being Reused:

1. In the CommCell Browser, navigate to the Assigned Media Pool. The contents of the Assigned Media pool are displayed in the right pane of the Browser.
2. From the right pane, right-click the media that you want to reuse, and then click **Allow Reuse**.

   Note that this option will be available only if the media was previously prevented from being reused.
3. In the Scratch Media Group Selection dialog box, select the scratch pool to which you want to move the media when the media is recycled.
4. Click **OK** to save the information.

Discover Media

Topics | How To | Related Topics

OVERVIEW

Before using a new media, the MediaAgent must collect certain information about it through a process known as discovery. When a media has been discovered its information is entered into the CommServe database. The media information is permanently retained; media does not have to be rediscovered if it is exported from the library and re-imported.

If new media are imported through a library's mail slot, the import operation triggers a discover operation. This is dependent on whether you have enabled or disabled the **Enable Auto-Discover** option for the library. (For more information on this option, see Library Properties - Media tab.)

- If the automatic discovery option is not enabled, the system will prompt you to provide the necessary details for the media.
- If the automatic discovery option is enabled, the system discovers the media during a subsequent inventory update triggered by a job from the CommCell.

If the automatic discovery option is not enabled for the library and if you have some undiscovered media from a previous import, or if you import new media by opening the library door and inserting them, you must initiate a discover operation.

Media can be discovered from both the **Library and Drive Configuration** window and the **CommCell Browser**.

DISCOVER CLEANING MEDIA

When you discover cleaning media, the system automatically assigns it to the **Cleaning Media** pool.

Discover Media - How To

Topics | How To | Related Topics

DISCOVER MEDIA FROM THE COMMCELL CONSOLE

You can use the following procedure to:

- Discover all media within a library
- Discover a partial set of media within a library

Required Capability: Capabilities and Permitted Actions

To discover media within a library:

1. From the CommCell Browser, right-click the library whose media you want to discover, and then click **Discover Media**.
2. If one or more new media are discovered, the system displays the Discover New Media dialog box and prompts you for media information.
3. Select the hardware type of the new media from the **New Media Type** list and the scratch pool to which you want the media assigned from the **Destination Scratch Pool** list.
4. The total number of undiscovered media available in the library is displayed in the **No. of media in Free Media Pool** field. Specify the number of media

you would like to discover in the **No. of media to be discovered** field.

5. Click **OK**.

You can also discover the media from the **Library and Drive Configuration** window. See Discover Media from the Library and Drive Configuration Window for more information.

DISCOVER A SPECIFIC MEDIA WITHIN A LIBRARY

Required Capability: Capabilities and Permitted Actions

➨ To discover a specific media within a library:

1. From the CommCell Browser, locate the library whose media you want to discover in the **Libraries** level.
2. Navigate to the **Media in Library** pool.

   All the media available in the library is displayed in the right-pane of the CommCell Console.

   Right-click the (undiscovered) media and then click **Discover**.
3. From the Discover New Media dialog box, select the Media Type and Scratch Pool to which the media must be moved.
4. Click **OK**.

The media is discovered and assigned to the specified scratch pool.

DISCOVER MEDIA FROM THE LIBRARY AND DRIVE CONFIGURATION WINDOW

Required Capability: Capabilities and Permitted Actions

➨ To discover media within a library:

1. Display the Library and Drive Configuration window.
2. Right-click the library whose media you want to discover, and then click **Discover Media**.
3. From the Discover New Media dialog box, enter the necessary information.
4. Click **OK**.
5. The system displays a warning message advising you to move the cleaning media to the Cleaning Media Pool. Click **OK**.

   If new media are discovered, they are assigned to the designated scratch pool. Otherwise, a message appears informing you that no new media were found.

You can also discover the media from the CommCell Console. See Discovering Media from the CommCell Console for more information.

ENABLE AUTOMATIC MEDIA DISCOVERY DURING LIBRARY CONFIGURATION

Required Capability: Capabilities and Permitted Actions

➨ To discover media within a library:

1. Display the Library and Drive Configuration window.
2. Detect the devices. Use Detection or Exhaustive Detection as required.
3. Configure the library as described in Configure Devices.

   During the configuration process, if the library has a barcode reader, the **Discover Media Options** dialog box is displayed.

   Perform one of the following:

   - To automatically discover the media in the library, select the default media type and then click **Yes**.
   - To manually discover the media, click **No**. See Discover Media from the CommCell Console for step-by-step instructions on manually discovering media in a library.

     Ensure that media is discovered, before using the library for a data protection operations.

   If the library does not have a barcode reader, another **Discover Media Options** dialog box is displayed.

   Select the correct media type available in the library and then click **OK**.

ENABLE OR DISABLE AUTOMATIC MEDIA DISCOVERY

Required Capability: See Capabilities and Permitted Actions

➡ To enable automatic media discovery:

1. From the CommCell Browser, right-click the library for which you wish to enable automatic media discovery, and then click **Properties**.
2. Click the Media Usage tab.
3. From the **Auto-Discovery of Media** region, click **Enable Auto-Discovery of Media into default scratch pool** option. (Clear this check box to disable this option.)
4. Select the default media type available in the library from the **Default Media Type** list.

   Note that the media available in a library must be compatible with the drives attached to the library.
5. Click **OK** to save the changes.

   When you subsequently import media, the imported media is automatically moved to the default scratch pool.

DISCOVERING CLEANING MEDIA

➡ To discover cleaning media within a library

1. From the CommCell Browser, right-click the library in which you want to discover cleaning media, and then click **Discover Cleaning Media** from the short-cut menu.
2. In the Discover Cleaning Media dialog box that appears, select the hardware type of the new media from the **Cleaning Media Type** list and the scratch pool to which you want the media assigned from the **Destination Cleaning Media Pool** list. Enter the number of media you want to import in **No. of media to be discovered** box.
3. Click OK.

   The newly imported cleaning media is displayed in the **Cleaning Media** pool.

DISCOVER MEDIA IN A BLIND LIBRARY

Required Capability: See Capabilities and Permitted Actions

➡ To discover media in a blind library:

1. From the CommCell Console, right-click the media you wish to discover and then click **Discover Media**.

   The system attempts to discover the media and reports the success or failure of the operation in the **Event Viewer**.

   Note that the discover operation is displayed as an inventory job in the **Job Controller** window.

Erase Spare Media

Topics | How To | Related Topics

Overview

The erase spare media operation ensures that old data from removable media (tapes and optical platters) are not recoverable once the media is recycled. This is done as follows:

- On tapes, the On-Media-Label (OML) is over-written by a new OML to indicate the erased status.
- On Optical media, the platter is formatted and a new OML is written.

Only spare, retired and recycled media from tape and optical libraries can be erased. Note, however, that the erase media operation cannot be performed on disk and stand-alone drives. Once a media is erased by this operation, data cannot be retrieved using Media Explorer.

Note that the **Erase Spare Media** operation will not erase the following data:

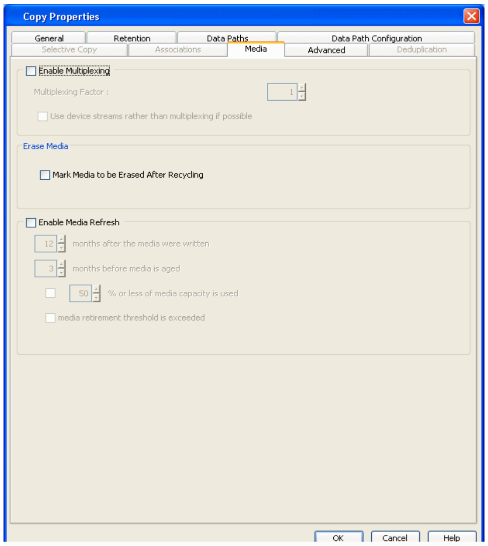
- Data associated with another CommCell, if the option to overwrite media from another CommCell is disabled in the **Media** tab of the **Library Properties** dialog box.
- Data written by other applications, if the option to overwrite media when content verification fails is disabled in the **Media** tab of the **Library Properties** dialog box. For more information on this option, see Library Properties - Media tab.

The Erase Media operation is a low priority job, and is displayed in the **Job Controller** window. It can be killed, if necessary.

Marking Media as Erasable

The first step in erasing spare media is to ensure that the media is marked for erase, when the media is recycled. This can be done from the **Media** tab of the **Storage Policy Copy** dialog box.

Enable the **Mark Media on to be Erased After Recycling** option to mark the media as erasable, once all the data in the media is pruned and the media is recycled.



□ Enable Multiplexing

Multiplexing Factor : 1

□ Use device streams rather than multiplexing if possible

Erase Media

□ Mark Media to be Erased After Recycling

□ Enable Media Refresh

12 months after the media were written

3 months before media is aged

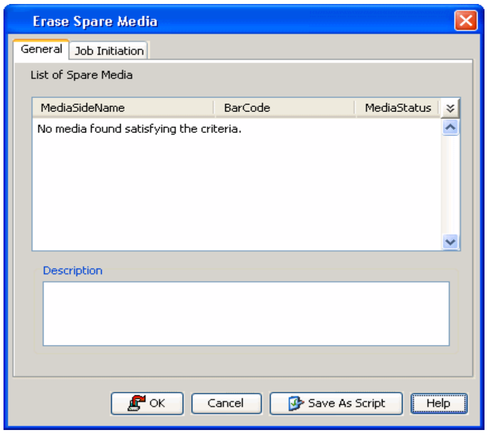
□ 50 % or less of media capacity is used

□ media retirement threshold is exceeded

Initiating a Spare Media Erase Operation

The **Erase Spare Media** operation erases spare media that are marked as erasable by a storage policy copy. This operation can be performed immediately or scheduled. This can be done from the Erase Spare Media dialog box.

All spare media that are marked as erasable and available within the library are displayed in this dialog box.

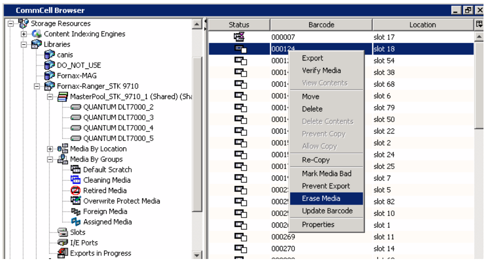


List of Spare Media

MediaSideName	BarCode	MediaStatus
No media found satisfying the criteria.		

Description

Erasing Spare or Retired Media



A specific spare or an retired media can also be erased immediately from the CommCell Console. This can be by done by the selecting the Erase Media option for the media.

More than one spare or retired media can be erased in a single operation by selecting multiple spare media and choose the Erase Media option for the selected media.

Alerts and Reports

Several alerts and reports can be established for the Erase Media operation. See Alerts and Monitoring for more information.

Back to Top

Erase Spare Media - How To

Topics | How To | Related Topics

Mark Spare Media for Media Erase Operation

To mark spare media for media erase operation:

1. From the CommCell Browser, right-click the storage policy copy for which you wish to erase the associated media, and then click **Properties**.
2. Click the Media tab.
3. Click the **Mark Media to be Erased After Recycling** option.
4. Click **OK**. The information is saved.

NOTES

When this option is enabled, the recycled media from this specific storage policy copy will be erased by the Media Erase operation.

ERASE SPARE MEDIA

To erase spare media:

1. Mark the media to be erased as described in Mark Spare Media for Media Erase Operation.
2. Run the Erase Spare Media operation. This can be done in one of the following ways:
   - Run the Erase Spare Media operation, immediately from the library level, as described in Run a Erase Spare Media Operation Immediately.
   - Schedule an Erase Spare Media operation from the library level, as described in Schedule an Erase Spare Media Operation.
   - Erase a specific spare or retired media, as described in Erase a Specific Spare or Retired Media.

RUN A ERASE SPARE MEDIA OPERATION IMMEDIATELY

Before You Begin

- Ensure that the spare media in the library have been marked as erasable, as described in Mark Spare Media for Media Erase Operation.

To run a erase spare media operation immediately:

1. From the CommCell Browser, right-click the library from which you wish to perform the spare media erase operation, and then click **Erase Spare Media**.
2. The Erase Spare Media dialog box displays a list of spare media that are marked as erasable, and available in the library.
3. Click **OK**.

   You can track the progress of the Erase Spare Media operation in the **Job Controller** window.

NOTES

When a media is erased, the following actions are performed on removable media:

- On tapes, the On-Media-Label (OML) will be over-written by a new OML, when the media is recycled.
- On Optical media, the platter will be formatted and a new OML will be written.

ERASE SPARE OR RETIRED MEDIA

Before You Begin

- Ensure that the media you wish to erase is available in the library. (not exported)

To erase spare or retired media:

1. From the CommCell Browser, right-click the spare or retired media that you wish to erase.

   To erase multiple media in a single operation, select the desired spare or retired media. Hold the Control key down to select more than one media.
2. Right-click and then select **Erase Media**.
3. Click **Yes** in the Confirm prompt asking you whether you wish to erase the media.

   You can track the progress of the Erase Media operation in the **Job Controller** window.

NOTES

When a media is erased, the following actions are performed on removable media:

- On tapes, the On-Media-Label (OML) will be over-written by a new OML, when the media is recycled.
- On Optical media, the platter will be formatted and a new OML will be written.

SCHEDULE A ERASE SPARE MEDIA OPERATION

Before You Begin

- Ensure that the spare media in the library have been marked as erasable, as described in Mark Spare Media for Media Erase Operation.

To schedule a erase spare media operation:

1. From the CommCell Browser, right-click the library from which you wish to perform the spare media erase operation, and then click **Erase Spare Media**.
2. The Erase Spare Media dialog box displays a list of spare media that can be erased.
3. Click **Schedule**.
4. From the Schedule Details (Schedule Details) tab of the **Schedule Details** dialog box, select the scheduling options that you want to apply.

5. Click **OK,** to submit the job for scheduling, .

NOTES

When a media is erased, the following actions are performed on removable media:

- On tapes, the On-Media-Label (OML) will be over-written by a new OML, when the media is recycled.
- On Optical media, the platter will be formatted and a new OML will be written.

Identifying Media Icons

The following table identifies the various media icons that may be displayed within a library and also identifies the operations that can be performed on each of these media.

Icons: Tape Libraries													
Icons: Optical Libraries^		N/A											
Media Status **Options**	Spare media	Cleaning media	Assigned media (active)	Assigned media (full)	Bad Media	Retired Media	Prevent Export	Undiscovered media	Media with duplicate barcodes	Media from a different library#	Appendable Media	Aged Media	Aged Retired Media
*** Load Media**	X		X	X	X	X	X				X	X	X
*** Export**	X	X	X	X	X	X		X	X		X	X	X
*** Verify Media**	X		X	X	X	X	X	X			X	X	X
View Contents			X	X	X		X				X	X	X
Move	X											X	
Delete	X	X				X						X	
Delete Contents			X	X	X		X				X		
*** Erase Media**	X					X						X	
Mark Media Bad	X	X	X	X			X				X	X	
Mark Media Full			X				X				X		
Mark Appendable				X	X								
*** Discover**								X					
*** Discover as Cleaning Media**								X					
*** Prevent Export/Allow Export**	X	X	X	X	X	X	X				X	X	X
Update Barcode	X	X	X	X	X	X	X				X	X	X
Properties	X	X	X	X	X	X	X				X	X	X

^ *Optical libraries include Optical platter, UDO & DVD media types.*

***** *Not Applicable for stand-alone drives.*

# *Depending on the status of the media (i.e., Assigned, Appendable, Bad, Full, etc), the options associated with that status are available.*

The following table lists media icons that are displayed in the `Find Media` dialog box which is displayed when you select the `List Media` Option from the Backup Set level in the CommCell Browser

Icon	**Description**
	Media in the library
	Media outside the library.

Media By Groups

Topics | How To | Related Topics

SCRATCH POOLS

A scratch pool is a repository of media that are available for use. For comprehensive information on scratch pools and the default scratch pool, see Scratch Pools.

CLEANING MEDIA

The Cleaning Media pool is the logical repository for the cleaning media in the library. For comprehensive information on cleaning media and cleaning media pools, see Cleaning Media.

RETIRED MEDIA

The Retired Media pool is the logical repository for all **Deprecated** media. Media is marked as **Deprecated** when the recycled spare media has been marked as **Bad** or exceeds the preset thresholds defined for the media in Media Expiration Threshold Parameters. The system determines whether a media is **Deprecated** during the following operations:

- Whenever a job requires spare media from the scratch pool, the system determines whether the media has exceeded its threshold values. If the threshold values are exceeded, it is marked as **Deprecated** and directly moved to the **Retired Media** pool.
- In the case of an active media, the system determines whether the media has exceeded its threshold values before writing to that media. If the threshold values are exceeded, an **Event Message** is generated indicating that the media has exceeded its threshold values. Such media are moved to the **Retired Media** pool until the media is recycled.
- Bad media is moved to the **Retired Media** pool after the media is recycled.
- If a cleaning media is marked bad or exceeds the preset thresholds defined for the media in the Media Expiration Threshold Parameters, it is marked as **Deprecated** and moved to the **Retired Media** pool.

You can perform the following operations on the media available in the **Retired Media** pool:

- Export a media to physically remove it from the library.
- Delete a media to remove the media information from the CommServe database. If the media you wish to delete is not already exported, the delete operation has an option to export the media before deleting it.
- Verify the media to confirm whether the media information displayed in the CommCell Console matches the OML in the media.

OVERWRITE PROTECT MEDIA

The Overwrite Protect Media pool is logical repository for media that should not be used for any write operations. The Overwrite Protect Media pool can be used to save media containing aged data, so that the aged data can be restored if necessary. (See Accessing Aged Data for more information.)

Note that only spare media can be moved to the Overwrite Protect Media pool. If you wish to save data from media in the Assigned Media pool, use the **Prevent Reuse** option to automatically move the media to a designated Overwrite Protect media pool when the media is recycled.

Note, however, that the guaranteed way of retaining data is setting the right Data Retention Rules or using the Retain the Job option on the Storage Policy Copy.

You can perform the following operations on the media available in the **Overwrite Protect Media** pool:

- Export a media to physically remove it from the library.
- View the contents of the media. This feature can be used to view information associated with the data secured by data protection operations residing in the

media.

- Verify the media to confirm whether the media information displayed in the CommCell Console matches the OML in the media.
- Delete the contents of the media.
- Mark a media bad.
- Prevent the media from being exported.
- Update the barcode associated with the media
- View the media properties

FOREIGN MEDIA

The Foreign Media pool is the logical repository for media that are not used by the MediaAgents in this CommCell. This could be media from another CommCell or backup software. This media pool can be used to manage foreign media using VaultTracker.

You can perform the following operations on the media available in the **Foreign Media** pool:

- Export a media to physically remove it from the library.
- Verify the media to confirm whether the media information displayed in the CommCell Console matches the OML in the media.
- Delete the media.
- Mark a media bad.
- Prevent the media from being exported.
- Erase the media
- View the media properties

ASSIGNED MEDIA

The Assigned Media pool is the logical repository for all used media inside or outside the library.

You can perform the following operations on the media available in the **Assigned Media** pool:

- Export the media to physically remove it from the library. After the export operation the media will be displayed both in the **Assigned Media** pool as well as the **Exported Media** pool.
- View the contents of the media. This feature can be used to view information associated with the data secured by data protection operations residing in the media.
- Verify the media to confirm whether the media information displayed in the CommCell Console matches the OML in the media.
- Delete the contents of the media.
- Mark an active media full.
- Mark a media bad.
- View the media properties

Back to Top

Media By Groups - How To

Topics | How To | Related Topics

Load Media

- Load a Media to a Drive

Export Media

- Export a Specific Media

View Contents

- View the Contents of a Media

Move Media

- Move a Media From One Scratch Pool to Another
- Move Media in Bulk From One Scratch Pool to Another

Delete Media

- Delete a Media

Delete Contents

- Delete the Contents of a Media

Erase Media

- Erase Spare Media

Discover Media

- Discover Media from the CommCell Console

Mark Media Bad

- Mark a Media Bad

Mark Media Full

- Mark a Media Full

Mark Media Appendable

- Marking a Media as Appendable
- Reuse Media Marked as Appendable

Media Chunk and Block Size

- Set the Chunk Size for Each Agent
- Set the Chunk Size and Block Size for a Data Path

Prevent Reuse

- Prevent an Assigned Media From Being Reused
- Reuse an Assigned Media that was Prevented From Being Reused

---

LOAD A MEDIA TO A DRIVE

Required Capability: Capabilities and Permitted Actions

➧ To load a media to a drive:

1. In the left pane of the CommCell Browser, click the **Media in Library** node.

   All the media available in the library are displayed in the right-pane.

2. From the right pane of the CommCell Browser, right-click the media that you want to load into a drive, and then click **Load Media**.

   The **Load Media** option will be displayed only for those media that are available in the library.

3. From the Load Media dialog box specify the resources that must be used to load media into a drive.

4. Click **OK**.

   The system will attempt to load the media into the specified drive. A event message is displayed in the **Event Viewer** after the successful completion of the operation.

EXPORT A SPECIFIC MEDIA

Required Capability: Library Management

➧ To export a specific media:

1. From the CommCell Console select the media you wish to export from one of the following pools or dialog boxes:
   - **Media in Library** (discovered and undiscovered media) pool
   - **Scratch pools**
   - **Cleaning Media** pool
   - **Retired Media** pool
   - **Assigned Media** pool

- **Media List** dialog box which appears when you select the **View Media** option that appears when you right-click a Storage Policy copy.
- **Media List** dialog box which appears when you select the **Change Data Path** option that appears when you right-click a Storage Policy copy.
- **Media Used By Job ID** dialog box which appears when you select the **View Media** option from the **Data Protections Job History**, **Backup Job History,** or **Data Migration History** windows.

2. Right-click the media that you want to export, and then click **Export.**
3. In the **Export Media** dialog box, enter an optional description of the location outside the library where the media will be stored.
4. Click **OK.**

   The location field is for display purposes only, to help you keep track of exported media. The MediaAgent has no control over media once they leave the library; it is your responsibility to ensure that exported media are stored in the location entered.

5. An **Export Media** prompt appears, prompting you remove the media. Do one of the following:
   - If you are exporting through a mail slot, click **OK**, wait for the media to be moved to the mail slot, and then remove them from the library.
   - If you are removing media directly, click **OK**, open the library door, remove the media that you want to export, and then close the door.

VIEW THE CONTENTS OF A MEDIA

Required Capability: Capabilities and Permitted Actions

To view the contents of a media

1. From the CommCell Browser, in the Media in Library pool or the Assigned Media pool, right-click the media for which you wish to view the content, and then click **View Contents**.

   or

   From the Media Used By Job ID dialog box right-click the media for which you wish to view the content, and then click **View Contents**.

2. Click **Yes** in the prompt which displays that the operation may take a few minutes.
3. The Contents of Media dialog box displays the details of jobs available in the media.

MOVE A MEDIA FROM ONE SCRATCH POOL TO ANOTHER

Required Capability: See Capabilities and Permitted Actions

To move a media from one scratch pool to another:

1. In the left pane of the CommCell Browser, select the scratch pool containing the media that you want to move. The contents of the scratch pool are displayed in the right pane of the Browser.
2. From the right pane of the CommCell Browser, right-click the media that you want to move, and then click **Move**.
3. In the Move Media dialog box, select the scratch pool to which you want to move the media. If it is cleaning media, select Cleaning Media pool.
4. Click **OK** to complete the transfer.

   The selected media is reassigned to the destination scratch pool.

MOVE MEDIA IN BULK FROM ONE SCRATCH POOL TO ANOTHER

Required Capability: See Capabilities and Permitted Actions

To move a number of unspecified media from one scratch pool to another:

1. From the CommCell Browser, right-click the scratch pool from which you want to move media (i.e., the source pool), and then click **Move Media** from the short-cut menu.
2. In the Move Media dialog box, enter the number of media to be moved in the **No. of Media to be moved** field. Select the scratch pool into which you want to move the media from the **Destination Scratch Pool** list.
3. Click **OK** to complete the transfer.

   The selected media is reassigned to the destination scratch pool.

DELETE A MEDIA

Required Capability: Capabilities and Permitted Actions

➨ To delete a media

1. In the CommCell Browser, right-click the media you wish to delete, and then click **Delete** Media.
2. Click **Yes** in the prompt asking you to confirm whether you wish to delete the media.
3. From the Delete Contents and Move Media dialog box, select the scratch pool to which you wish to move the media.
4. Click **OK** to save the information.

   The media information is deleted in the CommServe database and moved to the specified scratch pool.

DELETE THE CONTENTS OF A MEDIA

Required Capability: Capabilities and Permitted Actions

> **Caution**
>
> Once deleted, the contents of the media are not available for data recovery operations, and the system will not automatically force the next data protection operation to be a full backup. If you delete the contents of the media, you should immediately run a full backup for all the subclients associated with the media once the operations is complete.

1. In the left pane of the CommCell Browser, select the **Assigned Media** node.

   All the assigned media are displayed in the right-pane.
2. From the right pane of the CommCell Browser, right-click the desired media and select **Delete Contents**.

   NOTES

   The **Delete Contents** option will be displayed only for those media that are available in the library.
3. Click **Yes** to confim. The Enter Confirmation Text dialog displays.
4. Type "erase and reuse media" in the field, and click **OK**.
5. Select the name of the scratch pool to which the media must be moved, after the contents are deleted.
6. Click **OK**.
7. Click **OK** in the warning prompt to continue with the operation.

   The media information is deleted from the CommServe database and the media is moved to the specified scratch pool.

   The operation is recorded in the Audit Trail.

ERASE SPARE MEDIA

➨ To erase spare media:

1. Mark the media to be erased as described in Mark Spare Media for Media Erase Operation.
2. Run the Erase Spare Media operation. This can be done in one of the following ways:
   - Run the Erase Spare Media operation, immediately from the library level, as described in Run a Erase Spare Media Operation Immediately.
   - Schedule an Erase Spare Media operation from the library level, as described in Schedule an Erase Spare Media Operation.
   - Erase a specific spare or retired media, as described in Erase a Specific Spare or Retired Media.

DISCOVER MEDIA FROM THE COMMCELL CONSOLE

You can use the following procedure to:

- Discover all media within a library
- Discover a partial set of media within a library

Required Capability: Capabilities and Permitted Actions

➨ To discover media within a library:

1. From the CommCell Browser, right-click the library whose media you want to discover, and then click **Discover Media**.
2. If one or more new media are discovered, the system displays the Discover New Media dialog box and prompts you for media information.
3. Select the hardware type of the new media from the **New Media Type** list and the scratch pool to which you want the media assigned from the **Destination Scratch Pool** list.
4. The total number of undiscovered media available in the library is displayed in the **No. of media in Free Media Pool** field. Specify the number of media you would like to discover in the **No. of media to be discovered** field.
5. Click **OK**.

You can also discover the media from the **Library and Drive Configuration** window. See Discover Media from the Library and Drive Configuration Window for more information.

MARK A MEDIA BAD

Required Capability: Capabilities and Permitted Actions

To mark a media as bad:

1. In the CommCell Browser, right-click the media you wish to mark as bad, and then click **Mark Media Bad**.
2. Click **Yes** in the prompt asking you to confirm whether you wish to mark the media bad.

   The media status is changed to bad. (Media status can be viewed in the <*Media ID*> tab of the **Media Properties** dialog box.)

MARK A MEDIA FULL

Required Capability: Capabilities and Permitted Actions

To mark a media as full:

1. In the CommCell Browser, from the Media in Library pool or Assigned Media pool, right-click the active media you wish to mark as full, and then click **Mark Media Full**.

   or

   From the Media Used By Job ID dialog box right-click the media you wish to mark as full, and then click **Mark Media Full**.
2. Click **Yes** in the prompt asking you to confirm whether you wish to mark active media full.

   The media status is changed to full. (Media status can be viewed in the <*Media ID*> tab of the **Media Properties** dialog box.)

MARK A MEDIA AS APPENDABLE

Required Capability: Capabilities and Permitted Actions

To mark a media as appendable:

1. In the CommCell Browser, from the Media in Library pool or Assigned Media pool, right-click the exported media you wish to mark as appendable, and then click **Mark Appendable**

   or

   From the Media Used By Job ID dialog box right-click the media you wish to mark as appendable, and then click **Mark Appendable**.
2. Click **Yes** in the prompt asking you to confirm whether you wish to mark the media as appendable.

   The media status is changed to *Appendable* with the reason stating `User marked appendable`. (Media status can be viewed in the <*Media ID*> tab of the **Media Properties** dialog box.)

REUSE MEDIA MARKED AS APPENDABLE

Required Capability: See Capabilities and Permitted Actions

To reuse media marked as appendable:

1. From the CommCell Browser, right-click the library for which you wish to reuse media marked as appendable, and then click **Properties**.
2. Click the Media tab.
3. Click **Use Appendable Media within n Day (s) of its last write time**.

4. Type the number of days that the media can be used after it was marked as appendable.
5. Click **OK** to save the changes.

SET THE CHUNK SIZE FOR EACH AGENT

To set the chunk size:

1. From the **Tools** menu in the CommCell Console, click **Control Panel.**
2. Double-click **Media Management**.
3. Click the Chunk Size tab.
4. Click the Agent for which you wish to modify the chunk size, and modify the chunk size in the **Chunk Size** column.
5. Click **OK** in the **Media Management Configuration** dialog box to save the changes.

SET THE CHUNK SIZE AND BLOCK SIZE FOR A DATA PATH

Required Capability: See Capabilities and Permitted Actions

To set the chunk size and block size for a data path:

1. From the CommCell Browser, right-click the storage policy copy for which you wish to add the data paths, then click **Properties**.
2. Click the Data Paths tab.
3. Select a data path and then click the **Properties**.
4. You can view or modify the chunk and block size from the Data Path Properties dialog box.

PREVENT AN ASSIGNED MEDIA FROM BEING REUSED

Required Capability: See Capabilities and Permitted Actions

To prevent an assigned media from being reused:

1. In the CommCell Browser, navigate to the Assigned Media Pool. The contents of the Assigned Media pool are displayed in the right pane of the Browser.
2. From the right pane, right-click the media that you want to prevent reuse, and then click **Prevent Reuse**.

   Note that this option will be available only if the media was previously NOT prevented from being reused.
3. In the Overwrite Protect Media Group Selection dialog box, select the specific Overwrite Protect Media pool to which you want to move the media when the media is recycled.
4. Click **OK** to save the information.

REUSE AN ASSIGNED MEDIA THAT WAS PREVENTED FROM BEING REUSED

Required Capability: See Capabilities and Permitted Actions

To Reuse an Assigned Media that was Prevented From Being Reused:

1. In the CommCell Browser, navigate to the Assigned Media Pool. The contents of the Assigned Media pool are displayed in the right pane of the Browser.
2. From the right pane, right-click the media that you want to reuse, and then click **Allow Reuse**.

   Note that this option will be available only if the media was previously prevented from being reused.
3. In the Scratch Media Group Selection dialog box, select the scratch pool to which you want to move the media when the media is recycled.
4. Click **OK** to save the information.

Media By Location

Topics | Related Topics

MEDIA IN LIBRARY

The Media in Library pool is the logical repository for all media available in the library. See Identifying Media Icons for a list of media that may be available in the library and the operations that can be performed on each of these media. From the CommCell Console, you can view the properties such as the media status, barcode, library, location, last write time, and size of stored data for the media listed in this pool.

From the **Media in Library** pool in the CommCell Console, you can export media in bulk, based on a list or on a criteria. For comprehensive information on exporting media, see Export Media.

Only exported media will not be displayed in this list. See Media Operations for additional information on media options.

Media in Library pool is not applicable for Stand-Alone drives.

MEDIA WITH DATA MARKED FOR EXTENDED RETENTION

Media containing data that are marked extended retention is displayed with the suffix (E). This will help you identify media containing data marked for extended retention. See Tape Handling for more information.

UNDISCOVERED MEDIA

Undiscovered media are media that are available inside the library, but not yet discovered for by the MediaAgent. If an undiscovered media contains a valid barcode, the discover media operation provides you with the option to either discover the media or export the media. If an undiscovered media has no barcode or contains an invalid barcode (where the library could not read the barcode) only the slot ID for the media is displayed in the CommCell Console. Such media can only be exported.

MEDIA WITH DUPLICATE BARCODES

When two media with the same barcode are available in a library or different libraries, one of them must be exported in order to use the other media. In such a situation, it may be necessary to determine which media must be retained or exported.

Consider the following:

- Both media are undiscovered

  Both these media will be displayed in the **Media in Library** pool. As both these media cannot be discovered and used in the CommCell, export one and discover the other.

- One media is already a spare media (does not contain any data)

  Both these media will be displayed in the **Media in Library** pool, but the spare media will also be displayed in the original scratch pool. From the scratch pool, note the slot number of the original media. From the **Media in Library** pool, export the duplicate media residing on a different slot number/library.

- One media is an assigned media (contains data)

  Both these media will be displayed in the **Media in Library** pool, but the assigned media will also be displayed in the **Assigned Media** pool. From the **Assigned Media** pool, note the slot number of the media. From the **Media in Library** pool, export the duplicate media residing on a different slot number/library. Perform a verify media operation on the media.

In all these situations, the exported media can be re-introduced after changing the bar code label to contain a unique number. If, however, the exported media is stored, make sure that the duplicate barcode label is removed to avoid future mistakes.

In the case of media containing duplicate barcodes in two different libraries, after exporting one of the media from a library, the other library may not update its status until an inventory is performed. Hence, it is recommended that you perform the **Full Scan** or **Reset Library** operation.

MEDIA FROM A DIFFERENT LIBRARY

When more than one library with the same media type are attached to a CommCell, media belonging to one library may accidentally be inserted in another library. In such a situation, one of the following actions will be performed:

- If the media is a spare media which was exported from the original library, the media is automatically moved to the default scratch pool of the library in which the media resides. All media information will be removed from the original library. However, the media properties and history will be retained and displayed in the new library.
- If the media is an assigned media which was exported from the original library, the media will be displayed as a media from a different library. You will not be able to discover such a media. In such a situation, export the media and make sure that it is either imported back to its original library, or if stored, labeled properly.

Data can be restored from the media, if the media resides in a different library with compatible drive types.

EXPORTED MEDIA

The Exported Media pool is the logical repository for all media which were previously discovered and subsequently exported from the library. For comprehensive information on the Exported Media pool and Export Media see Export Media.

Back to Top

Find Media

Topics | How To | Related Topics

You can search for a media associated with the libraries available in the CommCell. You can search for a media using either the media’s barcode or unique ID. When the media is found, the **Media Properties** dialog box is displayed, which contains useful information for the media.

Find Media

Topics | How To | Related Topics

FIND MEDIA

Required Capability: Capabilities and Permitted Actions

➧ To find media:

1. From the CommCell Browser, right-click **Storage Resources** and then click **Find Media** from the shortcut menu.
2. In the **Find Media** dialog box, enter the barcode or unique ID of the media.
3. Click **Search**.

   If the media is found, the **Media Properties** dialog box is displayed. This dialog box displays the **Library** and **Location** information for the media.

Media Labeling

Proper media labeling is essential to media access and identification, both inside and outside libraries.

The MediaAgent software supports regular tape/optical libraries with barcode scanners in which specific barcode formats/patterns are required for different library models.

As stand-alone drives cannot read barcodes, manually entering media names in the CommServe database and physically marking or attaching barcode labels on media cartridges is highly recommended.

The MediaAgent also writes on-media labels (OML) on media during media initiation process to ensure correct media identification during subsequent access.

AVOIDING MEDIA LABELING ERRORS

In order for media to be accessible to the CommCell, the barcode or identifying name must be unique within the CommCell. A given barcode cannot be reused even if the media to which it was originally attached is physically removed from the library, unless it is deleted from the CommCell database.

If barcode labels are used, they should be compatible with the library’s barcode reader (see the library manufacturer’s documentation for a list of compatible labels) and properly affixed to the media (right side up and in the correct location).

For non-barcode media, proper labeling of the media as soon as it is exported is recommended. This will aid later in correctly identifying a media, when an import is requested.

Media Recycling

OVERVIEW

The MediaAgent automatically recycles media that no longer contains data by moving them back to the original scratch pool for re-use. In the case of magnetic storage devices, the MediaAgent physically removes the folders and files, if possible.

Media can be recycled when you prune data using the Data Aging operation or job based pruning in the CommCell. However, keep in mind, that data aging or job based pruning does not recycle media with an **Active** status. (If you wish to perform data recovery operations from data that has been aged or save the media containing the data for future use, see Accessing Aged Data.)

Media will also be recycled when you delete the following entities in the CommCell, if they are no longer valid or required and then perform an data aging operation:

- Storage policy or storage policy copy
- Client’s backup set
- Uninstall the Client or Agent

For comprehensive information on the Data Aging operation, see Data Aging.

Additionally, media is immediately recycled when you use the **Delete Content** option from the CommCell Console. For more information on the Delete Content option, see Delete Contents.

Data aging removes the data entries in the CommServe database to logically remove the data from the media. Once the data entries are removed from the CommServe database, data is logically removed and hence no longer available for restore.

TAPE OR OPTICAL MEDIA

> Data aging and recycling of optical media is similar to tape media, except that in the case of optical media, data from both sides of the media has to be removed in order to recycle an optical cartridge.

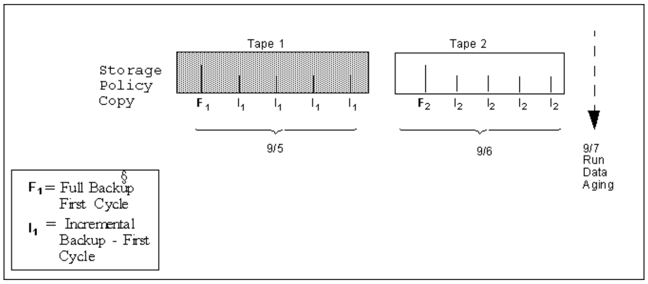
If data stored on media meets its retention criteria and data aging is run, the data is logically deleted (i.e., removed from the CommServe database). If all of the data on a media is pruned, the media is recycled. That is, it is returned to the scratch pool that is currently associated with the storage policy copy containing the media.

Let us look at the following examples, to gain a better understanding of recycling tape media:

RECYCLABLE MEDIA

In this example, **subclient A** has its first cycle on **Tape 1** and the second cycle on **Tape 2.** The data retention rule for the storage policy copy used by **Subclient A** has been set to one day and one cycle.

If data aging is run on **9/7**, all the data in **Tape 1,** (which exceeds the 1-day and 1-cycle criteria) will be aged and the media will be recycled.

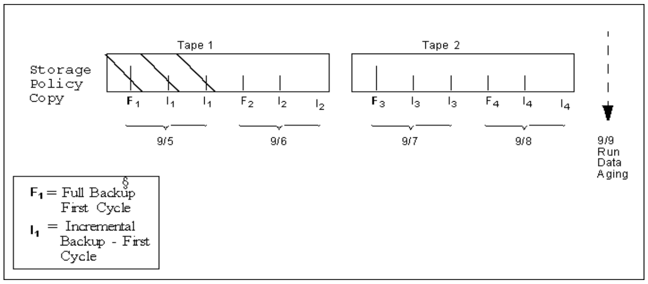


NON-RECYCLABLE MEDIA

In the following example, **Subclient A** has its first and second cycles on **Tape 1**, and the third and fourth cycles on **Tape 2**. The data retention rule for the storage policy copy used by **Subclient A** has been set to two days and three cycles.

If data aging is run on 9/9, only the first cycle can be aged in order to keep three cycles.

Because the second cycle is still on **Tape 1**, this tape cannot be recycled.


Tape 1
Tape 2
Storage Policy Copy
F_1 I_1 I_1 F_2 I_2 I_2
F_3 I_3 I_3 F_4 I_4 I_4
9/5
9/6
9/7
9/8
9/9 Run Data Aging
F_1 = Full Backup First Cycle
I_1 = Incremental Backup - First Cycle

DISK MEDIA

If data stored on disk media is deleted or pruned, the data is both logically and physically deleted. If the data aging operation cannot access data stored on disk for any reason (e.g., a disk sector is corrupt, data has been moved or deleted, a network connection is down, etc.) data will remain, but not be usable. You must manually remove the data through the operating system. The disk data is stored in the **CV_Magnetic** folder of the mount path.

List Media (Media Prediction)

Topics | How To | Support | Related Topics

Choose from the following topics:

Overview

List media option is useful to predict media required for the following operations:

- To restore data associated with a specific backup set, subclient or instance
- To restore the index required to browse data associated with a specific backup set or subclient
- To restore a specific file (or specific files and folders)
- To restore data associated with a specific job

Media prediction is useful in a variety of circumstances, including the following:

- To ensure that media required by an operation is available in the library, especially if you are restoring/recovering data across a firewall.
- In cases where data spans across several media, to identify the exact media necessary to restore/recover a file/folder/sub-section of the data.
- To identify and restore/recover from a copy that accesses a faster disk media rather than slower tape/optical media.
- To identify media associated with an alternate copy, when the media containing data associated with a specific copy is not readily available due to the following reasons:
  - When the media is exported from the library
  - When the media is used by another operation

Note that List Media operations are supported only with traditional browse and not with search results.

How to Perform a List Media Operation

The list media operation can be performed in several different ways, depending on the requirement. The following sections describe each of these methods.

LIST MEDIA ASSOCIATED WITH A SPECIFIC BACKUP SET, INSTANCE OR SUBCLIENT

This operation is referred to as **List Media** in the CommCell Console and provides the following options:

- Search media associated with the latest data protection cycle, starting from the latest full backup. (This is the default option.)
- Search media associated with data protection operations performed between a specified time range.
- Search for media associated with a specific storage policy copy, with the specified copy precedence number.

Keep in mind that when you search media from a secondary copy, the listed media may not reflect the entire instance or backup set data, unless all the storage policies associated with all the subclients have been configured for secondary copies.

The List Media option is available as a right-click option in the subclient level and in the **Browse Options** dialog box from the Backup Set/Instance level. See Perform List Media for a Subclient and Perform List Media for a Backup Set or Instance for step-by step instructions.

LIST MEDIA ASSOCIATED WITH INDEX

When a browse operation is performed, the system automatically restores the index from the appropriate media, if the index for the data is not available in the index cache, for Agents that support index. In such situations, this option is useful to verify the following:

- Whether the index is available in the index cache or must be restored from a media
- Whether the index must be restored from a media, if the appropriate media is available

The List Media option for index restore is available in the **Browse Options** dialog box. See List Media Associated with Index for step-by-step instructions.

Related Topics: Index

LIST MEDIA AND SIZE ASSOCIATED WITH SPECIFIC FILES AND/OR FOLDERS

This operation is referred to as **List Media and Size** in the CommCell Console and is useful to precisely predict media in which specific files or folders reside. For example:

- When a data protection operation spans across multiple media and you would like to know the exact media in which the files you wish to restore reside.
- You have a specific set of files (either a random set or a specific set, such as *.doc or *.txt) that you wish to restore and would like to know the all the media in which the files reside.
- You wish to restore a specific version of the file and would like to know the specific media in which the version resides.

> If you wish to exclude indexing media which does not contain data by using List Media and Size, create the `skipIndexingMedia` registry key and set the value to 1.

The List Media option for specific files and/or folders can be accessed from the Browse window, after selecting the appropriate files/folders for restore. See List Media and Size for Specific Files and/or Folders for step-by step instructions.

The precise media prediction is also available when you view different versions of the file (See Browse Multiple Versions of a File or Object) or when you use the find operation (see Find a File / Directory / Object) to locate a file.

LIST MEDIA ASSOCIATED WITH A SPECIFIC JOB

The Restore by Jobs feature provides the facility to restore data from a specific data protection operation. This option also includes the facility to list media associated with the job.

See List Media for specific Jobs for step-by step instructions.

RECALL MEDIA

The Recall Media feature provides the facility to temporarily bring media back from an export location for a specific operation and return the media to the export location when the operation is complete. This capability is useful if you have exported media to another location with the intention of keeping the media at the export location for an established period of time, but need to bring the media back from the export location for a specific purpose (such as a data recovery operation) prior to the original return date.

See Recall Media using List Media (Media Prediction) for step-by-step instructions.

GENERAL INFORMATION

Other notable features provided by the list media operation are:

- Facility to Print or Save the prediction results. The files can be saved either as a tab (.xls) or comma (.csv) separated file.
- The List Media and Size operation can be run immediately or scheduled. When it is run immediately the results are displayed immediately in the CommCell Console and if it is scheduled the results are saved in a specified file.

  Note that in both cases the result provides information on the total space required to restore the selected data.
- The List Media and Size operation also includes the ability to email prediction results by generating an alert (if configured) which would in turn contain the prediction results.
- Command line interface provides commands for some of the list media operations. See Command Line Interface - qlist for more information.
- The list media operation is displayed as a job (with appropriate controls, such Suspend, Resume, and Kill) in the Job Controller. Appropriate event messages are also populated in the Event viewer.
- The List Media and Size operation will not be supported if the MediaAgent used for the operation is not upgraded to the current software version.

Back to Top

List Media (Media Prediction) - How To

Topics | How To | Support | Related Topics

LIST MEDIA FOR A SUBCLIENT

Required Capability: See Capabilities and Permitted Actions

To list media for a subclient:

1. From the CommCell Browser, right-click the subclient for which you wish to list media and then click **List Media**.
2. From the List Media dialog box choose one of the following options:
   - Click **Media For the Latest Data** to list media associated with the most recent data protection cycle.
   - Click **Specify Time Range** to list media associated with data protection operations up to the specified date and time range.

     Use the **Data Before** box to specify the end date and time.
   - Click **Advanced** and then click **Exclude Data Before** to list media associated with data protection operations after the specified date and time.

   Note that you can use the **Specify Browse Time** and **Exclude Data Before** options to list media between a specified date and time range.
3. Click **OK**.

   The appropriate media is listed in the Media dialog box.

LIST MEDIA FOR A BACKUP SET OR INSTANCE

Required Capability: See Capabilities and Permitted Actions

To list media for a backup set or instance:

1. From the CommCell Browser, right-click the backup set or instance for which you wish to list media, click **All Tasks** and then click **Browse**.
2. From the Browse Options dialog box, if required, select the following options:
   - Click **Browse the Latest Data** to list media associated with the most recent data protection cycle.
   - Click **Specify Browse Time** to list media associated with data protection operations up to the specified date and time range.
     Use the **Browse Data Before** box to specify the end date and time.
   - Click **Advanced** and then click **Exclude Data Before** and then select the date and time from which you wish to list media associated with data protection operations.

   Note that you can use the **Specify Browse Time** and **Exclude Data Before** options to list media between a specified date and time range.
3. Click **List Media**.
4. From the List Media dialog box, click **List Media for restore within specified time range** and click **OK**.

   The appropriate media is listed in the Media dialog box.

LIST MEDIA ASSOCIATED WITH INDEX

Required Capability: See Capabilities and Permitted Actions

To list media associated with Index:

1. From the CommCell Browser, right-click the backup set or instance for which you wish to list media, click **All Tasks** and then click **Browse**.
2. From the Browse Options dialog box, if required, select the following options:
   - Click **Browse the Latest Data** to list media associated with the most recent data protection cycle.
   - Click **Specify Browse Time** to list media associated with data protection operations up to the specified date and time range.
     Use the **Browse Data Before** box to specify the end date and time.
   - Click **Advanced** and then click **Exclude Data Before** and then select the date and time from which you wish to list media associated with data protection operations. Select the **Include Metadata** option if you wish to include media containing metadata information.

   Note that you can use the **Specify Time Range** and **Exclude Data Before** options to list media between a specified date and time range.
3. Click **List Media**.
4. From the List Media dialog box, click **List Media containing index required for browse** and click **OK**.

The appropriate media is listed in the Media dialog box.
Note that this dialog box, by default, only lists media when the index is not available in the index cache. Select the **Show all media containing index** option to view information on whether the index is available in the index cache.

List Media and Size for Specific Files and/or Folders

Required Capability: See Capabilities and Permitted Actions

To list media for specific files and/or folders:

1. From the CommCell Browser, right-click the backup set or instance for which you wish to list media, click **All Tasks** and then click **Browse**.
2. Select the appropriate options for browsing data from the Browse Options and Advanced Browse Options dialog box and then click **OK**.
3. From the browse window, depending on your requirement, perform any one of the following:
   - Expand the tree and select the file and or folders that you wish to restore and then click **List Media**.
   - If you wish to search and restore a specific file or specific set of files, use the Find option as described in Find a File/Directory/Object.
     The results are displayed in the lower pane of the **Find** window.
     Right-click the desired file or folder and then choose **List Media**.
   - If you wish to restore a specific version(s) of a file, use the View All Versions option as described in Browse and Restore File Versions.
     The results are displayed in the File Version Restore / All Versions dialog box.
     Right-click the desired version of the file and then choose **List Media**.
4. From the List Media dialog box, choose one of the following options:
   - Choose the **Immediate** option, to immediately display the media list in the Media dialog box.
   - Choose the **Schedule** option, to schedule the list media operation and then type (or browse and select) the file name (including the path) in which the results from the scheduled operation must be saved in the **Result file location on CommServe** box.

     Click **Configure** to select the appropriate schedule from the Schedule Details dialog box. Click **Options** to provide advanced scheduling options. Click **OK**. The results of the scheduled operation are stored in the specified file.
5. If necessary, you can configure an alert for the operation. Click **Advanced** to provide the alert details and click **OK**.
6. The List Media results provide a list of associated media and, detailed media and data information including the total space required (on destination disk) to restore selected data. The results from an immediate run are displayed on Media dialog box and Media Prediction report, however the scheduled results are available only in Media Prediction report located under AlertAttachments folder in the installation directory.

List Media for specific Jobs

Required Capability: See Capabilities and Permitted Actions

To list media for specific jobs:

1. Right-click the backup set for which you wish to list media, click **All Tasks** and then click **Restore by Jobs**.
2. If necessary, select the necessary options in the Restore by Jobs filter dialog box. Click **OK**.
3. In the Backup Job History dialog box, right-click the job for which you wish to list media and then click **Restore**.
4. In the General tab of the **Restore Options** dialog box, click **List Media**.

   The appropriate media is listed in the Media dialog box.

Back To Top

Media Properties

Topics | How To | Related Topics

General

Media Information

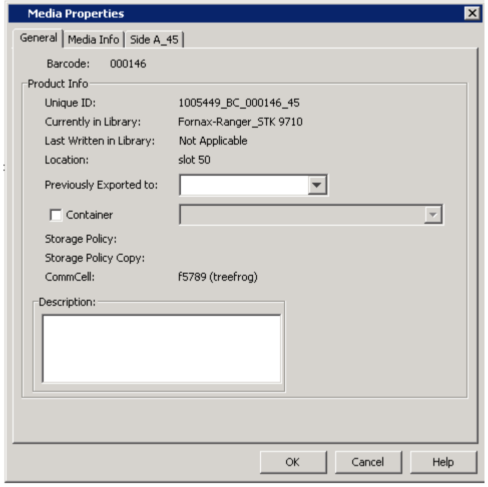
Media Properties (Unique ID)

- Status

GENERAL

The general information about a media, including the barcode, unique ID for the media in the CommCell, the current library, last written library, location in the library (slot number, or if mounted on a drive, the drive number), export location if the media is exported, the previous export location if the media was previously exported, the storage policy and storage policy copy accessing the media, the stream number (of the storage policy) that was used to write to the media and the CommCell ID are displayed.

The general information about a media can be viewed from the **General** tab of the **Media Properties** dialog box.



Barcode: 000146

Product Info

Unique ID: 1005449_BC_000146_45

Currently in Library: Fornax-Ranger_STK 9710

Last Written in Library: Not Applicable

Location: slot 50

Previously Exported to:

□ Container

Storage Policy:

Storage Policy Copy:

CommCell: f5789 (treefrog)

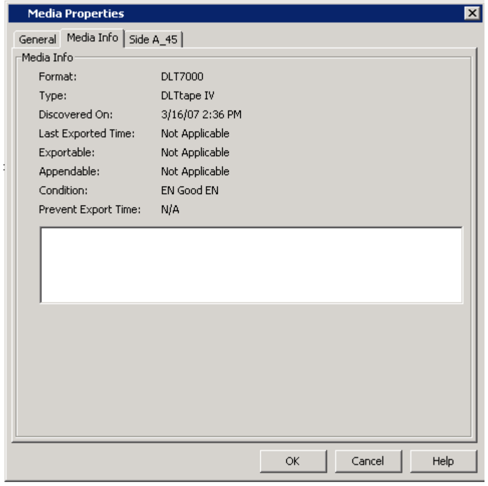
Description:

MEDIA INFORMATION

The general information about a media, including the recording format, the media type, discovery date and time, whether the media is required for auxiliary Copy, whether the media is appendable or not, export date and time (if exported), and the condition of the media and the data and time on which it was marked as prevent export, if the media was marked as prevent export is displayed.

The media information can be viewed from the **Media Info** tab of the **Media Properties** dialog box.

See View the Condition of a Media for step-by-instructions.



Media Info

Format: DLT7000

Type: DLTtape IV

Discovered On: 3/16/07 2:36 PM

Last Exported Time: Not Applicable

Exportable: Not Applicable

Appendable: Not Applicable

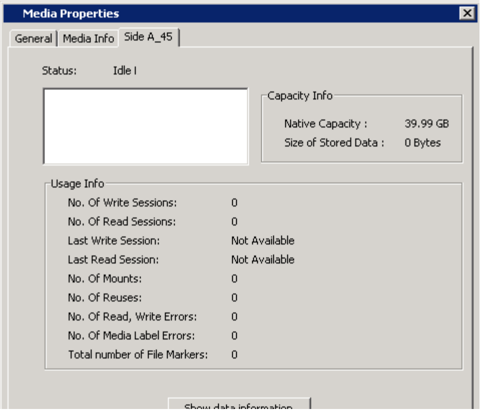
Condition: EN Good EN

Prevent Export Time: N/A

MEDIA PROPERTIES (UNIQUE ID)

The media information about a media, including information about the amount of data stored in the media and the usage information. The usage information is used to compare against the thresholds established for the media.

Information about the specific media can be viewed from tab that displays the unique ID of the media in the **Media Properties** dialog box. For optical media, two tabs representing the sides of the media the will be displayed. You can also view information on the data available in the media by clicking the **Show Data Information** button.



Status: Idle I

Capacity Info

Native Capacity : 39.99 GB

Size of Stored Data : 0 Bytes

Usage Info

No. Of Write Sessions: 0

No. Of Read Sessions: 0

Last Write Session: Not Available

Last Read Session: Not Available

No. Of Mounts: 0

No. Of Reuses: 0

No. Of Read, Write Errors: 0

No. Of Media Label Errors: 0

Total number of File Markers: 0

STATUS

The media is cycled through the following stages:

- When new media is imported and discovered in a library, it is assigned to a scratch pool.
- When a job requires a media, a media is logically reassigned to the Assigned Media pool.

- Subsequent jobs write data into the media until it is full. At this point, although the media cannot be written to, it remains in the Assigned Media pool, available for restore operations.
- When all of the data on the media exceeds its retention criteria and is pruned, the system returns the media to a scratch pool for reuse.
- Occasionally, a job may encounter hardware or software errors while attempting to write to or read from a media. In these cases, the system may mark the affected media as BAD so that the problem can be diagnosed and, if possible, fixed. (For additional information on scratch pools, see Master Drive Pools, Drive Pools and Drives.)

Status information about individual media is provided in the CommCell Console. Note that if a media is double-sided (e.g., an optical disk), each side has its own status. The table that follows lists the various media status with a brief description of each status:

Active	The media is available for writing. In other words, when data is sent to the storage policy copy associated with the media group containing this media, the data is written to this media.
Full	The MediaAgent can no longer write to this media, either because it contains no free space or because the media has been marked as full, either by the user or by the MediaAgent. The MediaAgent will mark a media full if it is unavailable for a data protection operation. However, the media will remain in the Assigned Media pool as it contains un-pruned data. (See Mark a Media Full for step-by-step instructions on marking media volumes full, .)
Idle	This media belongs to a scratch pool rather than to the Assigned Media pool. New media should have **Idle** status after they are imported and discovered.
Read Only	The MediaAgent may mark a media as **Read Only** when an error is encountered while attempting to write to the media. Although data cannot be written to a **Read Only** media, it will be possible to restore data from the media.
Bad	The MediaAgent can no longer read from nor write to this media. Media with **Bad** status will be moved to the **Retired Media** pool after it is recycled.
Appendable	An Appendable media typically has room left on it. The MediaAgent can write to this media, if the Mark Media **Appendable** option and **Use Appendable Media for (n) Days** option are enabled in the **Media** tab of **Library Properties**. (For more information on this option, see Library Properties.) Media is marked as Appendable in the following situations: ● When a media is found to be exported by a data protection or Auxiliary Copy job. ● When a media is stuck in a drive, by a data protection or Auxiliary Copy job. ● If the number of streams are reduced for a Storage Policy copy. ● If the **Start New Media** option is enabled for a backup from the **Advanced Backup Options** dialog box. ● If the **Start New Media** option is enabled for an auxiliary copy job from the **Auxiliary Copy** dialog box. ● Marked as full by the job to perform a LAN free data protection operation. ● If an alternate data path is used in a Storage Policy Copy. ● Marked as **full** by the user. ● Marked as Full to create a Synthetic Full.

Media Properties - How To

Topics | How To | Related Topics

VIEW THE CONDITION OF A MEDIA

To view the condition of a media:

1. From the CommCell Browser, right-click the media whose condition you wish to view and then click **Properties**.
2. The **Condition** option in the Media Info tab of the **Media Properties** dialog box displays information about the condition of the media.

VIEW THE STATUS OF A MEDIA

Required Capability: Capabilities and Permitted Actions

To view the status of a media:

1. From the CommCell Browser, click the media whose status you wish to view and then click **Properties**.
2. Click the <*Media ID*> tab.

   The **Status** option displays information about the status of the media.

VIEW THE MEDIA USAGE INFORMATION

To view the media usage information:

1. From the CommCell Browser, click the media whose usage information you wish to view and then click **Properties**.
2. Click the *<Media ID>* tab.

   The **Usage Info** area displays information about the usage information for the media.

Pop-up Messages Associated with Media Outside Library

The MediaAgent displays several messages when a job does not find the required media within the library. Such messages include the following:

- Event Messages in the Event Viewer.
- *Pop-up* messages in the MediaAgent Computer.
- In some cases, *Pop-up* messages in the CommCell Console. (The cases are indicated later in this section, as a table.)

These messages are displayed for a short period, every time the job is automatically re-tried until you import the requested media.

> All media operations associated with a stand-alone drive, including scheduled operations, display a pop-up message in all the CommCell Consoles and the MediaAgent computer, if the requested media is not mounted in the drive or if the drive is empty.
>
> In addition, for stand-alone drives, the jobs may or may not display some of these prompts for required media. This depends on the options selected in the Media tab of the **Library Properties** dialog box.

The following table provides a list of jobs and the associated operations when a requested media is not found within the library:

JOBS	**POP-UP MESSAGES**		**RESOURCE RESERVATION (DRIVE AND MEDIA)***
	MEDIAAGENT COMPUTER	**COMMCELL CONSOLE (ON ANY COMPUTER)**	
Data Protection Operations	NO	NO	NO
Data Recovery Operations	YES	YES - The CommCell Console from which the operation is initiated.** NO - For a NetWare MediaAgent.	NO
Index Restore -Browse	YES	YES - The CommCell Console from which the operation is initiated.** NO - For a NetWare MediaAgent.	NO
Index Restore -Data Protection Operations	NO	NO	NO
Auxiliary Copy			
Source	NO	NO	NO
Destination	NO	NO	NO
Synthetic Full			
Source	NO	NO	NO
Destination	NO	NO	NO
Scheduled Jobs	YES	NO	Depends on the type of job that is scheduled.

* - Resource reservation implies that the reserved resource, i.e., drive and media, will not be available for other CommCell operations with an equal or lesser priority, until the operation which reserved the resource completes or is killed by the user.

** - On a MediaAgent computer, if you have a CommCell Console open, you may see both the MediaAgent's message as well as the message in the CommCell Console.

Cleaning Media

Topics | How To | Troubleshoot | Related Topics

OVERVIEW

Several features to manage cleaning media is provided. The following sections provides a detailed discussion on the subject.

IMPORT CLEANING MEDIA

When you import a cleaning media, the system automatically assigns it to the cleaning media pool. For comprehensive information on importing see Import Media.

DISCOVER CLEANING MEDIA

When you discover cleaning media, the system automatically assigns it to the **Cleaning Media** pool.

CLEANING MEDIA POOL

The Cleaning Media pool is the logical repository for the cleaning media in the library. When you configure a library for the first time, the system creates a Cleaning Media pool for each library.

- Use the **General** tab of the **Cleaning Media Group Properties** dialog box to modify the following:
  - **Cleaning media pool name**: If necessary you can provide a descriptive name, for easier system administration.
  - **Low Watermarks:** You can establish a low watermark for the cleaning media pool. This parameter represents the minimum number of cleaning media that should be available in the cleaning media pool at all times. If the number of available cleaning media falls below the low watermark, the system logs a message in the **Event Viewer** and generates the **Insufficient Storage** alert, if configured. You can view the status of media available in the scratch pools by generating the **Scratch Pool** report.
- Use the **BarCode Patterns** tab of the **Cleaning Media Group Properties** dialog box to assign the barcode patterns for automatic identification of the cleaning media in the library. If the barcodes patterns are assigned and if the **Enable Auto-Discovery of media into default scratch pool** option is enabled in the **Library Properties** dialog box, cleaning media with matching barcodes will be automatically moved to the Cleaning Media pool. (For more information on the Enable Auto-Discovery of media into default scratch pool option, see Auto-Discover Media.)

  Consider the following when the automatic media discovery option is not enabled, or if you have not assigned the barcode patterns for cleaning media:

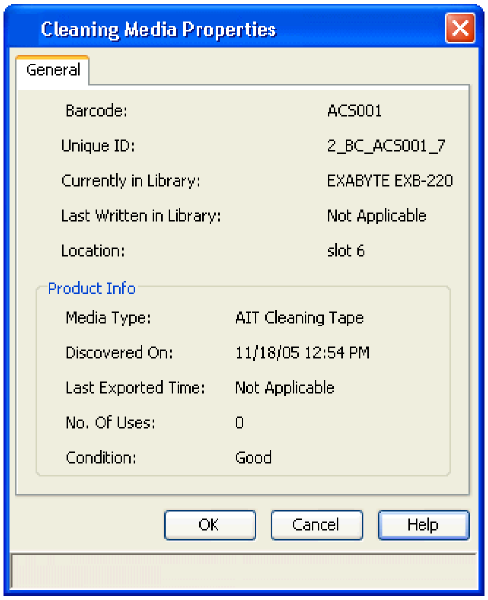
  - Make sure that the Cleaning Media pool contains only the cleaning media.
  - A cleaning media will be identified (and automatically moved to the Cleaning Media pool) when it is mounted in a drive during a drive validation or data protection operation only when the **Check for cleaning media loaded in the Drive** option is enabled in the Drive tab of **Library Properties** dialog box.

Cleaning media can be marked as **Bad**, if necessary.

Cleaning Media Pool is not applicable for Stand-alone drives.

CLEANING MEDIA PROPERTIES

The Media Properties provides general information about the cleaning media.



Cleaning Media Properties

General

Barcode: ACS001

Unique ID: 2_BC_ACS001_7

Currently in Library: EXABYTE EXB-220

Last Written in Library: Not Applicable

Location: slot 6

Product Info

Media Type: AIT Cleaning Tape

Discovered On: 11/18/05 12:54 PM

Last Exported Time: Not Applicable

No. Of Uses: 0

Condition: Good

Cleaning Media - How To

Topics | How To | Troubleshoot | Related Topics

Import Cleaning Media

Required Capability: Capabilities and Permitted Actions

> If you are not using a mail slot, be careful not to open the library door while media are mounted in drives within the library. In some library models (e.g., ATL 200, ATL 500) opening the door causes the library to unmount all media, even those that are in active use. This can cause database inconsistency and failure of the running job(s).
> Inserting media in and closing the mail slots of some libraries may trigger a full inventory operation (rather than an inventory update) .

To import cleaning media to the cleaning media pool

1. From the CommCell Browser, right-click the library for which you want to import the cleaning media, and then click **Import Cleaning Media**, from the short-cut menu.
2. An Import Media prompt appears, advising you to do one of the following:
   - If you are importing through a mail slot, insert one or more media into the mail slot and wait for them to be moved to storage slots. In many library types, you may also have to wait for the inventory to complete. Do not click OK until all of the imported media have been moved to storage slots and the inventory is completed.

     > If you click **OK** in the Insert Media prompt before the media are moved to storage slots and the inventory is completed, the MediaAgent will not discover the media. You must manually discover media as described in Discovering Cleaning Media.

     After all media are transferred to storage slots and the inventory is completed, click OK in the Import Media prompt.
   - If you are inserting media directly, open the library door, insert media into storage slots, and then close the door and wait for the inventory to complete. Click **OK** in the Import Media prompt and then discover the cleaning media. For more information, see Discovering Cleaning Media.

   When cleaning media is imported, the system assigns it in one of the following ways:

   - If the cleaning media is already catalogued, it belongs to the cleaning media pool.
   - If the cleaning media is not catalogued and is successfully discovered, the system displays the Discover Cleaning Media dialog box. Use this dialog box to assign the cleaning media to the cleaning media pool.
3. In the Discover Cleaning Media dialog box that appears, select the hardware type of the new media from the **Cleaning Media Type** list and the scratch pool to which you want the media assigned from the **Destination Cleaning Media Pool** list. Enter the number of media you want to import in **No. of**

media to be discovered box.

4. Click **OK**.

   The newly imported cleaning media is displayed in the **Cleaning Media** pool.

DISCOVERING CLEANING MEDIA

To discover cleaning media within a library

1. From the CommCell Browser, right-click the library in which you want to discover cleaning media, and then click **Discover Cleaning Media** from the short-cut menu.
2. In the Discover Cleaning Media dialog box that appears, select the hardware type of the new media from the **Cleaning Media Type** list and the scratch pool to which you want the media assigned from the **Destination Cleaning Media Pool** list. Enter the number of media you want to import in **No. of media to be discovered** box.
3. Click OK.

   The newly imported cleaning media is displayed in the **Cleaning Media** pool.

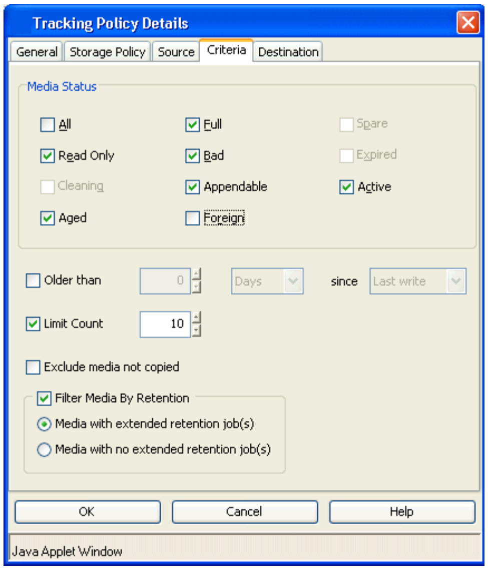
Tape Handling

Identifying Media with Extended Retention

This section provides information on how to identify and export tapes that contain data with extended retention.

If you have a VaultTracker license, you can define a tracking policy by selecting the **Media with extended retention job(s)** option in the **Criteria** tab of the **Tracking Policy Details** dialog box.

(See Create a Tracking Policy for step-by-step instructions.)



Media Status

☐ All ☑ Full ☐ Spare
☑ Read Only ☑ Bad ☐ Expired
☐ Cleaning ☑ Appendable ☑ Active
☑ Aged ☐ Foreign

☐ Older than 0 Days since Last write

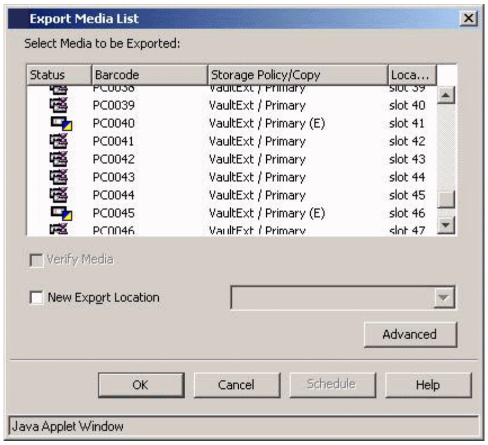
☑ Limit Count 10

☐ Exclude media not copied

☑ Filter Media By Retention
● Media with extended retention job(s)
○ Media with no extended retention job(s)

If you do not have a VaultTracker License, you can export media from a list. (See Export Media From a List for step-by-step instructions.) When you export media using a list, all media containing data with extended retention is displayed with the suffix (E) in the **Export Media List** dialog box as shown in the sample image on the right. You can use this information to select the appropriate media for export.

Also note that similar information is displayed when you view a list of media from the Media Library and Exported Media pools in the CommCell Browser.



Select Media to be Exported:

Status	Barcode	Storage Policy/Copy	Loca...
	PC0038	VaultExt / Primary	slot 39
	PC0039	VaultExt / Primary	slot 40
	PC0040	VaultExt / Primary (E)	slot 41
	PC0041	VaultExt / Primary	slot 42
	PC0042	VaultExt / Primary	slot 43
	PC0043	VaultExt / Primary	slot 44
	PC0044	VaultExt / Primary	slot 45
	PC0045	VaultExt / Primary (E)	slot 46
	PC0046	VaultExt / Primary	slot 47

☐ Verify Media

☐ New Export Location

Freeing Space on Media

This page provides information on how to figure out the reasons on why media or space is not getting freed up for re-use. Also there may be situations where you may want to forcibly age off data to free up media or disk for emergency re-use.

- Run the Data Retention Forecast and Compliance Report to see a list of data that are not prunable and the reasons.

  Hint: Select only those storage policy copies that you are interested in, as this report is time-consuming to generate.

- Run a Data Aging operation to age existing data that qualified for aging from the media. (See Data Aging for step-by-step instructions.)
- Check the Data Retention Rules established for the copies. (See Basic Retention Rules and Extended Retention Rules for more information.) If necessary, you can decrease the retention period to free up media space.

  Hint: Make sure to run a Data Aging operation to make the space available after reducing the retention period on any of the copies.

- Make sure that Auxiliary Copies are scheduled on a regular basis and that they have been successfully run. Data on the primary copy will not be aged off if Auxiliary Copies are not successful on the secondary copies. (See Start an Auxiliary Copy for step-by-step instructions and also generate the Auxiliary Copy Job Summary Report to see whether these jobs complete successfully.)
- If necessary you may also delete the contents of a media, (without running Data Aging) if you know that all of the data on a particular media is not required. (See Delete Contents for more information.)
- For Disk Libraries, you can also setup the Thresholds for Managed Disk Space which will automatically delete the old data. See Thresholds for Managed Disk Space for more information. Retentions on copies are still honored, so you may have to lower them alongside using this option.

Performance Tunables for Media Management

Topics | How To | Related Topics

The following sections describe some of the tunable parameters in Media Management that can be used to improve the performance.

INCREASING CHUNK SIZE

A chunk is the unit of data that the MediaAgent software uses to store data on media. For Sequential access media, chunk is defined as data between two file markers. The default chunk size for File System like data is 4 GB and for data associated with databases is 16 GB. For Random access media each chunk is a file on the disk. The default chunk size for this type of media is 2 GB.

This parameter will have an impact only when backing up to tape. A higher chunk size will give you better throughput. Recommended values are: 8 GB, 16 GB or 32 GB. However the disadvantage is that granular restores (e.g., single file restore) will be slower. On the other hand large restores, like a full machine rebuild will be a bit faster.

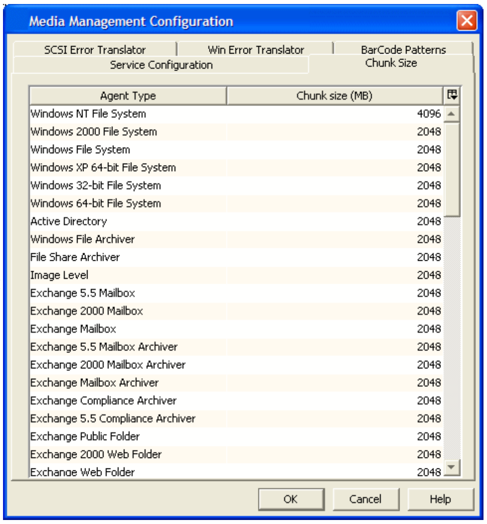
A lower value is recommended for frequent checks of slower data protection operations, especially when data is moving across a WAN link.

Chunk size is configurable using the **Chunk Size** tab of the **Media Management Configuration** dialog box, on a per application basis. The Media Management Configuration dialog box is accessible from the CommCell Console Control panel.(See Set the Chunk Size for Each Agent for step-by-step instructions.)

The chunk size established in this dialog box affects all data write operations in the CommCell. However you can establish the DMMBCHUNKSIZE registry key to control the chunk size of data write operations going to the MediaAgent in which the registry key is created. Note that if this registry key is created it will override the values established in this dialog box for that MediaAgent.

Also note that the values established for the NAS NDMP *i*DataAgents in this dialog box only apply to libraries attached to the MediaAgent using NDMP Remote Server. For libraries attached to a File Server, the system, by default, uses 4GB as the chunk size for file servers that support restartability (e.g., NetApp filer). For such file servers you can establish the nRESTARTWINDOWSIZE registry key to control the chunk size. For other file servers, the chunk size is based on the size of the tape used to backup the data and this is not configurable.

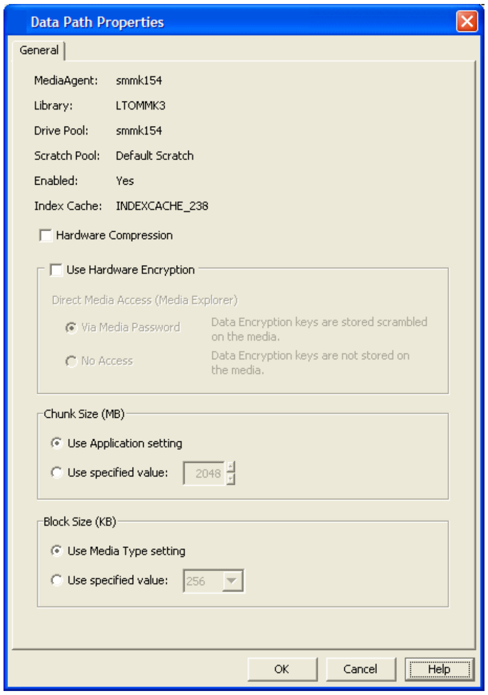
(The values in the **Chunk Size** tab of the **Media Management Configuration** dialog box applies only to tape media; for and optical media the system by default uses 2 GB as the chunk size.)



Agent Type	Chunk size (MB)
Windows NT File System	4096
Windows 2000 File System	2048
Windows File System	2048
Windows XP 64-bit File System	2048
Windows 32-bit File System	2048
Windows 64-bit File System	2048
Active Directory	2048
Windows File Archiver	2048
File Share Archiver	2048
Image Level	2048
Exchange 5.5 Mailbox	2048
Exchange 2000 Mailbox	2048
Exchange Mailbox	2048
Exchange 5.5 Mailbox Archiver	2048
Exchange 2000 Mailbox Archiver	2048
Exchange Mailbox Archiver	2048
Exchange Compliance Archiver	2048
Exchange 5.5 Compliance Archiver	2048
Exchange Public Folder	2048
Exchange 2000 Web Folder	2048
Exchange Web Folder	2048

Chunk Size can also be established from the **Data Path Properties** dialog box available from the **Data Paths** tab of the **Copy Properties** dialog box, for the specific data path. (See Set the Chunk Size and Block Size for a Data Path for step-by-step instructions.)

Chunk size established at the data path level overrides the chunk sizes established for the various Agents, as discussed in the preceding paragraph.



Data Path Properties

General

MediaAgent: smmk154

Library: LTOMMK3

Drive Pool: smmk154

Scratch Pool: Default Scratch

Enabled: Yes

Index Cache: INDEXCACHE_238

□ Hardware Compression

□ Use Hardware Encryption

Direct Media Access (Media Explorer)

● Via Media Password — Data Encryption keys are stored scrambled on the media.

○ No Access — Data Encryption keys are not stored on the media.

Chunk Size (MB)

● Use Application setting

○ Use specified value: 2048

Block Size (KB)

● Use Media Type setting

○ Use specified value: 256

INCREASING BLOCK SIZE

MediaAgents can write to media using different block sizes, if the Operating System associated with the MediaAgent in which the library is configured supports a higher block size. The system can write block sizes up to 256 KB and can automatically read block sizes up to 512 KB. If the block sizes are larger than 512 KB, read operations from the media will fail. Also note that such media will be over written and re-used if the **When Content Verification Failed** option is enabled in the **Library Properties (Media)** dialog box

Block sizes can be modified from the **Data Path Properties** dialog box available from the **Data Paths** tab of the **Copy Properties** dialog box, for the specific data path. (See Set the Chunk Size and Block Size for a Data Path for step-by-step instructions.)

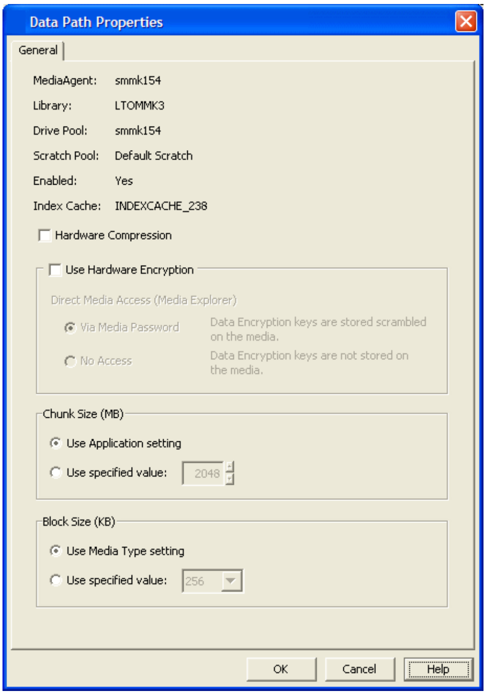
Higher block sizes on tape media are faster, but consider the following before increasing the block size:

- Note that the new block size must be supported by the HBA driver as well as by the tape drive. The most commonly used values are 128 KB or 256 KB.
- MediaAgents with direct attached SCSI devices on Windows 2000 do not support block sizes higher than 64 KB.
- NetApp NAS file servers for ONTAP 6.5.3 or later allow block sizes up to 256 KB, but NetApp servers for ONTAP 6.5.2 or earlier allow maximum block sizes of 64 KB.
- EMC Celerra NAS file servers support block sizes up to 128 KB.
- If you do specify a block size larger than the allowed limit, the NAS backup process automatically changes your entry to the maximum allowable block size.

For mount paths, block size is the buffer size used for each write operation. (The File system allocation unit size is decided at the time of formatting the volume.)

Cautions:

- All MediaAgents that share a storage policy must support the higher block size.
- If the MediaAgent that performs the restore is different than the original MediaAgent, then the destination MediaAgent must have HBA cards and drives to be able to read the higher block size.



Data Path Properties

General

MediaAgent: smmk154

Library: LTOMMK3

Drive Pool: smmk154

Scratch Pool: Default Scratch

Enabled: Yes

Index Cache: INDEXCACHE_238

□ Hardware Compression

□ Use Hardware Encryption

Direct Media Access (Media Explorer)

● Via Media Password — Data Encryption keys are stored scrambled on the media.

○ No Access — Data Encryption keys are not stored on the media.

Chunk Size (MB)

● Use Application setting

○ Use specified value: 2048

Block Size (KB)

● Use Media Type setting

○ Use specified value: 256

INCREASING JOB MANAGER UPDATE INTERVALS

The system, by default updates the Job Manager, every 5 minutes or whenever a chunk is closed, whichever is sooner. You can marginally improve the performance by increasing the job update interval when you increase the chunk size. However increasing the update interval will result in infrequent updates to the job progress in the Job Controller. These changes will not impact NAS NDMP *i*DataAgent backups.

(See Job Update Interval for more information on modifying the settings.)

CONFIGURE THE APPLICATION READ SIZE

Application read size is the size of the application data read from the clients for data transfer during backup operations. This parameter is defined for each subclient in the Storage Device (Data Transfer Option) tab. This value is set at 64 KB by default. Values for Application Read size must be in the power of 2; minimum value is 64 KB, maximum value is 4096 (4 MB).

Increasing the application read size will increase the rate of data transfer. Note that each application internally allocates a buffer size that is suitable for handling the application data. When the size of the application data read during backup operations matches the source application's internal buffer allocation then the overhead is minimized. So to achieve optimal rate of data transfer during backups, configure this value based on the source application's buffer allocation. See Set the Application Read Size for step-by-step instructions.

This configuration is supported for the following agents:

- Microsoft Windows File System *i*DataAgent
- Virtual Server *i*DataAgent
- Microsoft SQL Server *i*DataAgent

UNBUFFERED IO FOR LIBRARIES

When backing up to devices, you can enable **Use Unbuffered I/O** option in the **Mount Path Properties** dialog box to bypass the Windows file system buffering. Varying amounts of speedup will be observed depending upon the architecture of the disk. (See Use Unbuffered I/O for additional information.)

You can establish the `dwMaxAsyncIoRequests` registry key to control the number of read ahead buffers in the unbuffered I/O mode.

> The read streams for deduplication jobs are not **unbuffered**. Therefore, this registry key does not have an effect on deduplicated data and in completion of Auxiliary copy jobs of deduplication data sets.

DATA MULTIPLEXING

Multiplexing does not improve performance of an individual backup operation. However multiple backups run in parallel to a single tape drive, results in better utilization of the tape drives, especially when the backups are from slower clients. This helps in better overall throughput and reduction in the backup window.

For LAN backups, make sure that the network between the clients and MediaAgent is capable of supporting multiple simultaneous backups.

Do not over multiplex. That would be counter-productive and slow down the backups as well as restores. Multiplexing factor must be set equal to the ratio of tape drive throughput and client source speed. For example, if the tape drive has rated speed of 40 Mb/sec and clients are able to supply the data at about 12 Mb/sec, then a multiplexing factor of 3 is advisable. Typical multiplexing factor is between 2 and 5.

Also note that restores from multiplexed data are not slower.

See Data Multiplexing for complete details.

Back to Top

Performance Tunables for Media Management - How To

Topics | How To | Related Topics

SET THE CHUNK SIZE FOR EACH AGENT

To set the chunk size:

1. From the **Tools** menu in the CommCell Console, click **Control Panel.**
2. Double-click **Media Management**.

3. Click the Chunk Size tab.
4. Click the Agent for which you wish to modify the chunk size, and modify the chunk size in the **Chunk Size** column.
5. Click **OK** in the **Media Management Configuration** dialog box to save the changes.

SET THE CHUNK SIZE AND BLOCK SIZE FOR A DATA PATH

Required Capability: See Capabilities and Permitted Actions

➧ To set the chunk size and block size for a data path:

1. From the CommCell Browser, right-click the storage policy copy for which you wish to add the data paths, then click **Properties**.
2. Click the Data Paths tab.
3. Select a data path and then click the **Properties**.
4. You can view or modify the chunk and block size from the Data Path Properties dialog box.

SET THE APPLICATION READ SIZE

➧ To set the application read size:

1. From the CommCell Browser, right-click the subclient for which you wish to configure the application read size and then click **Properties**.
2. Select the **Storage Device** tab and the Storage Device (Data Transfer Option) tab within. Specify the desired read size in the **Application Read Size** field.
3. Click **OK** to save your changes.

ENABLE UNBUFFERED I/O ON A MOUNT PATH

Related Topic

- Use Unbuffered I/O

Required Capability: Capabilities and Permitted Actions

➧ To enable unbuffered I/O on a mount path:

1. From the CommCell Browser, right-click the mount path that you wish to enable unbuffered I/O, and then click **Properties**.
2. From the General tab of Library Properties, click the **Use unbuffered I/O** option.
3. Click **OK** to save the changes.

ENABLE DATA MULTIPLEXING

Before You Begin

Data Multiplexing cannot be enabled on a secondary copy, a copy of a disk library, or on a Disaster Recovery Backup storage policy.

Required Capability: Capabilities and Permitted Actions

➧ To enable data multiplexing:

1. From the CommCell Browser, right click the storage policy copy whose storage policy you want to enable data multiplexing, then click **Properties**.
2. From the Media tab of the **Copy Properties** dialog box, select **Enable Multiplexing**.
3. Select the number of subclients whose data will be multiplexed to the same media from the **Multiplexing Factor** list box.
4. Click **OK** to save your changes.

➧ To enable data multiplexing for Oracle jobs:

1. From the CommCell Browser, click **Job Management** from the **Control Panel** window.
2. From the Job Management (General) tab, select **Enable Multiplexing for Oracle**.
3. Click **OK** to save your changes.

Load Balancing Operations Between Libraries

OVERVIEW

The software system includes many features that help you to balance the operations between available storage resources in the CommCell. For example:

- You may find that a specific MediaAgent over loaded or slow and hence you may want to configure the MediaAgent in such a way that a only a specific number of jobs use the MediaAgent at any given time, while re-directing the overflow jobs to other MediaAgents in the CommCell.
- You may want more jobs to use a specific MediaAgent with a library that has faster and/or more number of drives, then MediaAgents with libraries that have slower and/ or fewer drives.
- You may want to utilize all storage resources in the CommCell, so that all data protection operations are completed in the specific operation window.

This document describes how to configure the MediaAgent software to distribute the load between multiple resources.

LOAD BALANCING USING THE LEAKY BUCKET MECHANISM

Using the leaky bucket mechanism each resource will be utilized until the threshold established for the resource is reached. When the thresholds are reached, the system automatically uses the next available resource.

Consider the following examples:

EXAMPLE 1:

This example illustrates how load balancing can be accomplished between 2 MediaAgents that share a library.

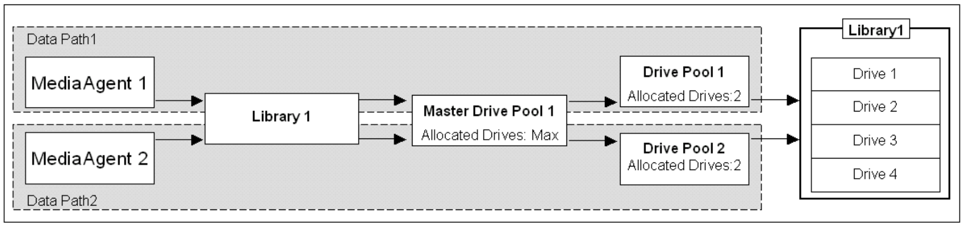
In this example, 2 MediaAgents (MediaAgent 1 and MediaAgent 2) are configured to share a library with 4 drives. Such a configuration would result in the following data paths:

- MediaAgent 1 -> Library 1 -> Drive Pool 1 -> 4 drives
- MediaAgent 2 -> Library 1 -> Drive Pool 2 -> 4 drives

To perform load-balancing between the 2 MediaAgents, you can allocate 2 drives for each of the MediaAgents. This can be done by as follows:

- Allocating 2 drives to each of the drive pools.
- Setting the criteria for using the alternate data path when resources are busy.

This ensures that jobs automatically switch-over to the next available resource, when the thresholds are reached.



In the above example, (assuming that several jobs are running concurrently at a given time) the first two jobs will use the resources in data path 1, while the third and fourth jobs use the resources in data path 2. Subsequent jobs in the queue will be routed to a data path with an available resource, as soon as a resource is freed.

EXAMPLE 2:

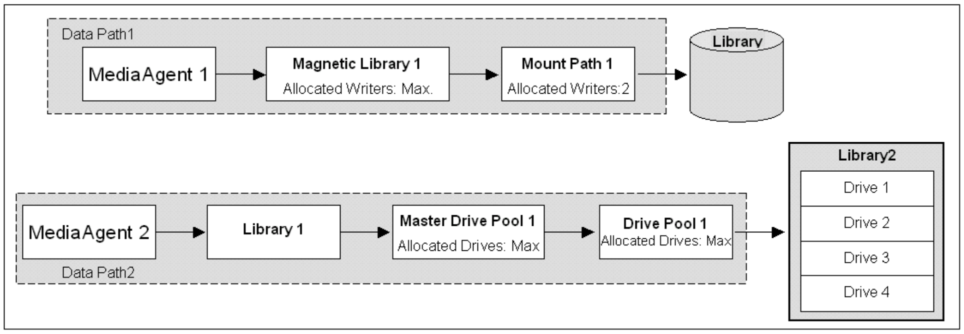
This example illustrates how load balancing can be accomplished between a tape library and a disk library.

In this example, MediaAgent 1 has a disk library configured, while MediaAgent 2 has a tape library. Such a configuration would result in the following data paths:

- MediaAgent 1 -> Disk Library 1 - >Mount Path
- MediaAgent 2 -> Tape Library 1 -> Drive Pool 1 -> 4 drives

To perform load-balancing between these 2 MediaAgents, in such a way that at any given time 2 jobs write to the disk library, while also using all the drives in the library. This can be done by as follows:

- Setting the maximum number of writers to 2 in the disk library.
- Allocating the maximum number of drives (4 in this example) in the drive pools associated with the tape library.
- Setting the criteria for using the alternate data path when resources are busy.



In the above example, (assuming that several jobs are running concurrently at a given time) the first two jobs will use the resources in data path 1, while the next four jobs use the resources in data path 2. Subsequent jobs in the queue will be routed to a data path with an available resource, as soon as a resource is freed.

Note that at any given time, the maximum number of jobs will be within the established threshold. (i.e., 2 for the disk library and 4, which is the maximum or the total number of drives in the tape library.)

Load Balancing Using Spill and Fill

The spill and fill method equally distributes the jobs among available resources.

The following example illustrates the spill and fill mechanism between tape and disk libraries:

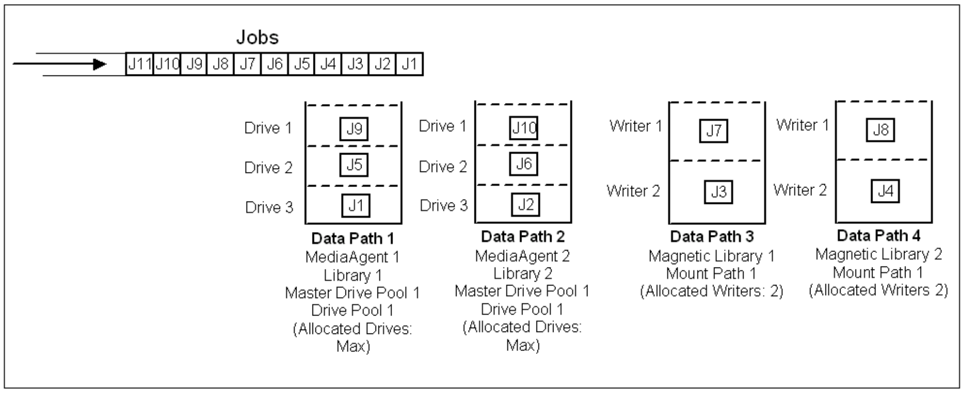
In this example, 2 MediaAgents have been configured with tape/optical libraries, while 2 more MediaAgents have 2 disk libraries configured. Such a configuration would result in the following data paths:

- MediaAgent 1 -> Tape Library 1 -> Drive Pool 1 -> 3 drives
- MediaAgent 2 -> Tape Library 2 -> Drive Pool 1 -> 3 drives
- MediaAgent 3 -> Disk Library 1 - >Mount Path 1
- MediaAgent 4 -> Disk Library 2 - >Mount Path 1

To perform load-balancing between these 4 MediaAgents, in such a way that at any given time 2 jobs write to the disk library, while using all the drives in the tape/optical libraries. This can be done by as follows:

- Setting the maximum number of writers to 2 in the disk libraries.
- Allocating the maximum number of drives (3 in this example) in the drive pools associated with the tape library.
- Setting the criteria for using the alternate data path as spill and fill .

This ensures that the jobs are distributed equally among all the MediaAgents.



See Also: Load balance (Spill and fill) between Data Paths.

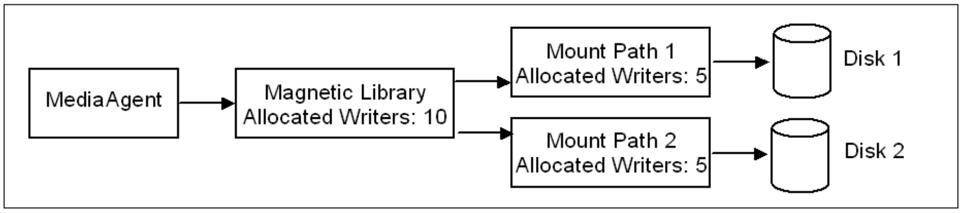
LOAD BALANCING BETWEEN DISK LIBRARIES

You can perform a simple load-balancing between 2 mount paths in a disk library, without using alternate data paths. This can be done using the **Mount Path Allocation Policy** in disk libraries and mount paths.

The following example illustrates this mechanism.

In this example, MediaAgent A has a disk library containing 2 mount paths. To perform load-balancing between these 2 mount paths, in such a way that at any given time 5 jobs write to the disk library, you can:

- Define the **Mount Path Allocation Policy** at the disk library to 10.
- Define the **Mount Path Allocation Policy** at each of the mount path to 5.



In the above example, (assuming that several jobs are running concurrently at a given time) the first five jobs will use mount path 1, and the next five jobs will use mount path 2. Subsequent jobs in the queue will be routed to either one of the mount paths, as soon as a mount path is freed.

Once the maximum allocated writers are used, the system will constantly check for an available resource, and as soon as one is freed the next job in the queue will be automatically routed to use that resource.

Back to Top

Hardware Changes

Topics | How To | Related Topics

OVERVIEW

In the course of using libraries and drives, you may have the need to either replace devices due to wear and tear, or add devices due to upgrade requirements. These replacements or additions must also be established within the MediaAgent so that the data stored in these libraries can be accessed after such additions or replacements. The How To sections describe the procedures that must be adopted while adding or replacing libraries and drives.

Hardware Changes - How To

Topics | How To | Related Topics

UPDATE THE FIRMWARE FOR LIBRARIES AND DRIVES

Before You Begin

- Verify and ensure that the firmware version that you wish to upgrade to is supported by MediaAgent.

  Contact your software provider to obtain the list of firmware versions supported for the device.

To update the firmware in a library

1. Verify and ensure that no jobs are in progress or scheduled to occur when the firmware is upgraded.
2. Note the current Operating System level mapping of devices regarding SCSI access path and address.
3. Stop the **MediaAgent Services** in all the MediaAgents that use the library.
4. Upgrade the firmware on the library based on guidelines provided by the hardware vendor.
5. Verify and ensure that the device comes back online correctly at the device level as instructed by the hardware vendor. Perform the necessary test operations that may be specified by hardware vendor.
6. Verify and ensure that the devices are visible to the operating system. Redetect the devices and compare the SCSI access path and address information noted in Step 2.
7. Start the **MediaAgent Services** in all the MediaAgents that use the library.

8. Once the devices come back **online** in the CommCell Console, run a test backup to see whether the devices function correctly.

CHANGE THE MEDIAAGENT (HOST) ASSOCIATED WITH A LIBRARY

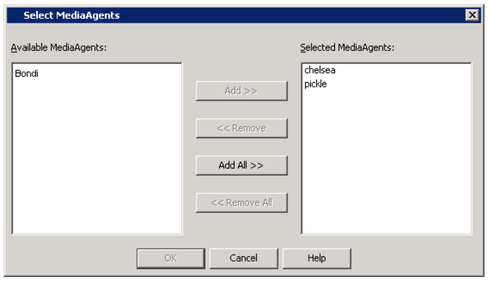
The following procedure outlines the steps involved in changing the MediaAgent associated with a library. Use this procedure when you attach the library to a different MediaAgent

TO CHANGE THE MEDIAAGENT ASSOCIATED WITH A LIBRARY

1. Detach the library from the old MediaAgent computer and attach it to the new MediaAgent computer.
2. Check and verify that the library and drives are visible to the operating system in the new MediaAgent computer.

   For a more detailed explanation on verifying the driver configurations, see Driver Configurations.
3. Display the Library and Drive Configuration window.

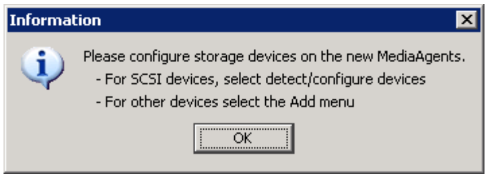
   Select only the old and new MediaAgents in the **Select MediaAgents** dialog box.



4. Click **OK** in the Information prompt.

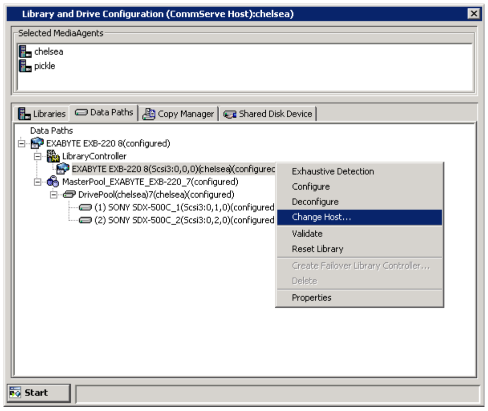
   This prompt is displayed as the library is not yet configured in the new MediaAgent.

   The system displays the library configured under the old MediaAgent.

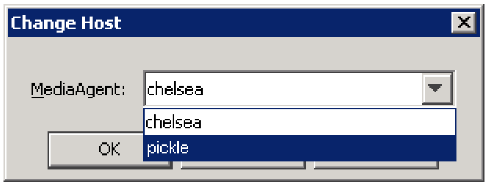


Please configure storage devices on the new MediaAgents.
- For SCSI devices, select detect/configure devices
- For other devices select the Add menu

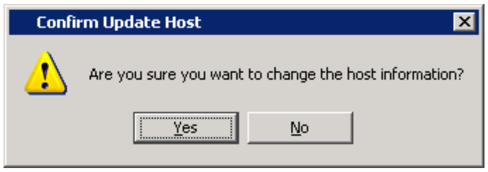
5. Right-Click the library controller and then choose **Change Host**.


Library and Drive Configuration (CommServe Host):chelsea)
Selected MediaAgents
chelsea
pickle
Libraries
Data Paths
Copy Manager
Shared Disk Device
Data Paths
EXABYTE EXB-220 8(configured)
LibraryController
EXABYTE EXB-220 8(Scsi3:0,0,0)(chelsea)(configurec
MasterPool_EXABYTE_EXB-220_7(configured)
DrivePool(chelsea)7(chelsea)(configured)
(1) SONY SDX-500C_1(Scsi3:0,1,0)(configured
(2) SONY SDX-500C_2(Scsi3:0,2,0)(configured
Exhaustive Detection
Configure
Deconfigure
Change Host...
Validate
Reset Library
Create Failover Library Controller...
Delete
Properties
Start

6. Select the name of the new MediaAgent to which the library is currently attached.

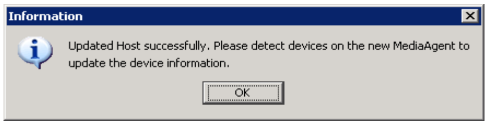


7. Click **Yes** in the confirm prompt.



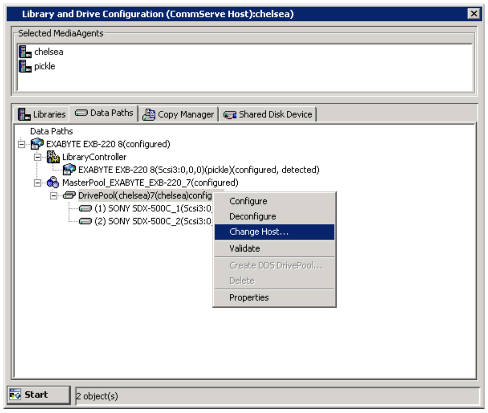
Are you sure you want to change the host information?

8. Click **OK** in the Information prompt.



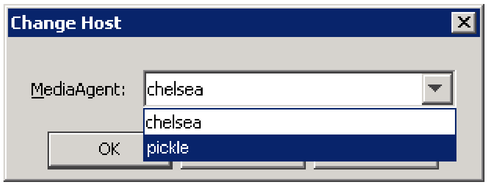
Updated Host successfully. Please detect devices on the new MediaAgent to update the device information.

9. Right-click the **DrivePool** and then choose **Change Host**.

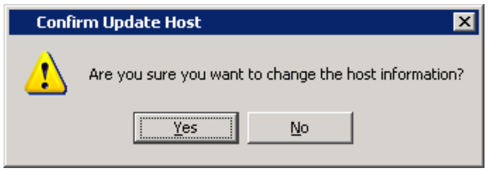


Library and Drive Configuration (CommServe Host):chelsea)
Selected MediaAgents
chelsea
pickle
Libraries
Data Paths
Copy Manager
Shared Disk Device
Data Paths
EXABYTE EXB-220 8(configured)
LibraryController
EXABYTE EXB-220 8(Scsi3:0,0,0)(pickle)(configured, detected)
MasterPool_EXABYTE_EXB-220_7(configured)
DrivePool(chelsea)7(chelsea)config
(1) SONY SDX-500C_1(Scsi3:0
(2) SONY SDX-500C_2(Scsi3:0
Configure
Deconfigure
Change Host...
Validate
Create DDS DrivePool...
Delete
Properties
Start
2 object(s)

10. Select the name of the new MediaAgent to which the library is currently attached.

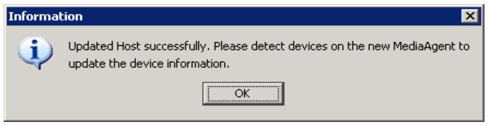


11. Click **Yes** in the confirm prompt.



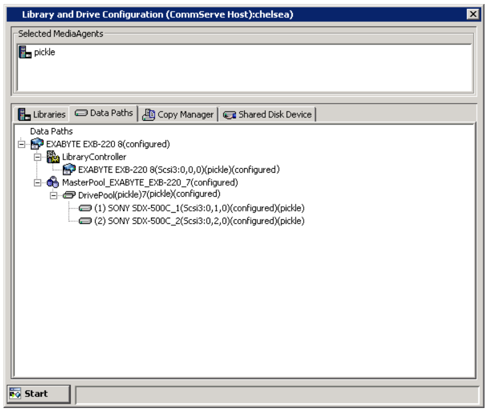
Are you sure you want to change the host information?

12. Click **OK** in the Information prompt.



Updated Host successfully. Please detect devices on the new MediaAgent to update the device information.

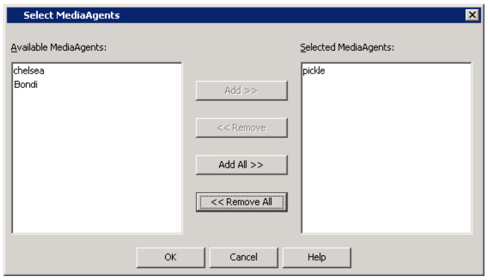
The system displays the library configured under the new MediaAgent.



Library and Drive Configuration (CommServe Host):chelsea)
Selected MediaAgents
pickle
Libraries
Data Paths
Copy Manager
Shared Disk Device
Data Paths
EXABYTE EXB-220 8(configured)
LibraryController
EXABYTE EXB-220 8(Scsi3:0,0,0)(pickle)(configured)
MasterPool_EXABYTE_EXB-220_7(configured)
DrivePool(pickle)7(pickle)(configured)
(1) SONY SDX-500C_1(Scsi3:0,1,0)(configured)(pickle)
(2) SONY SDX-500C_2(Scsi3:0,2,0)(configured)(pickle)
Start

13. From the **Start** Menu, click **Select MediaAgents**.

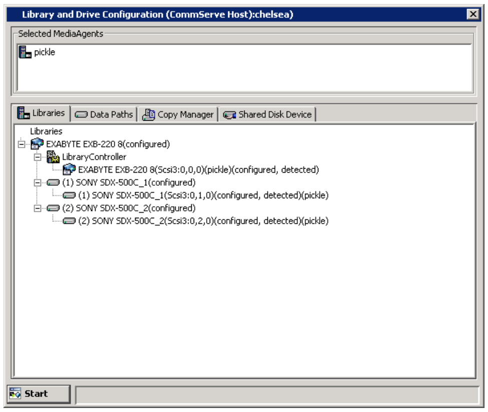
In the **Select MediaAgents** dialog box, select the name of the MediaAgent to which the library is currently attached.



14. Detect the devices as described in Detect Devices.

Once the detection process is complete, the devices should be displayed with `configured, detected` status.

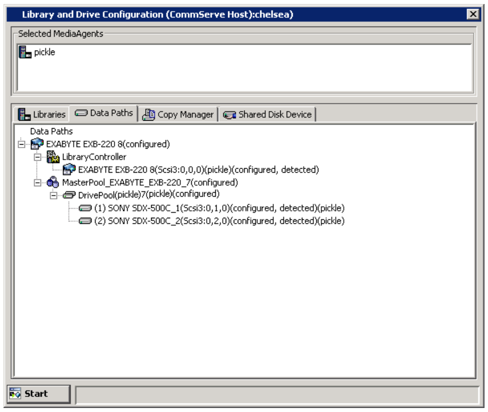
The **Library** tab provides the physical view of the devices (library and drives).



pickle

```
Libraries
EXABYTE EXB-220 8(configured)
    LibraryController
        EXABYTE EXB-220 8(Scsi3:0,0,0)(pickle)(configured, detected)
    (1) SONY SDX-500C_1(configured)
        (1) SONY SDX-500C_1(Scsi3:0,1,0)(configured, detected)(pickle)
    (2) SONY SDX-500C_2(configured)
        (2) SONY SDX-500C_2(Scsi3:0,2,0)(configured, detected)(pickle)
```

The **Data Paths** tab provides a logical view of the data path used to access the devices - library, master drive pool, drive pool, drive.



pickle

```
Data Paths
EXABYTE EXB-220 8(configured)
    LibraryController
        EXABYTE EXB-220 8(Scsi3:0,0,0)(pickle)(configured, detected)
    MasterPool_EXABYTE_EXB-220_7(configured)
        DrivePool(pickle)7(pickle)(configured)
            (1) SONY SDX-500C_1(Scsi3:0,1,0)(configured, detected)(pickle)
            (2) SONY SDX-500C_2(Scsi3:0,2,0)(configured, detected)(pickle)
```

UPDATE THE SCSI ADDRESS OF A CONFIGURED LIBRARY

Updating SCSI addresses in the CommServe database is not the same as changing the SCSI mapping of devices.

SCSI addresses must be *updated* on the CommServe database when the actual SCSI addresses of the devices change.
You may have to shut down and restart the machine whenever you add new devices. Make sure that the library and/or drives are visible to the operating system after the reboot.

To update the SCSI address of a configured library within the CommServe database

1. Open the **Service Control Manager** window in the MediaAgent machine in which the SCSI addresses have been changed.
2. **Stop** and **Restart** the MediaAgent Service in all the MediaAgents that use this library.
   - If the library has a serial number, the SCSI addresses will be automatically updated in the CommServe database.
   - If the library has no serial number, manually update the SCSI address in the **Library Properties and Drive Properties** dialog boxes, available in the **Library and Drive Configuration** window.

ADD NEW SLOTS TO A CONFIGURED LIBRARY

The following procedure outlines the steps involved in adding new slots to a previously configured library.

BEFORE YOU BEGIN

- The new slots added must be available in the library.

TO ADD NEW SLOTS TO A CONFIGURED LIBRARY

1. Display the Library and Drive Configuration window.
2. Select *all* the MediaAgents that share the library in the **Select MediaAgents** window and click **OK**.
3. Detect the devices as described in Detect Devices.
4. Configure the library as described in Configure Devices.

Replace a Library

The following procedure outlines the steps involved in replacing an existing library with a new library without deconfiguring the existing library.

BEFORE YOU BEGIN

- The new library should have the same drive type
- The number of drives in the new library must be the same or more

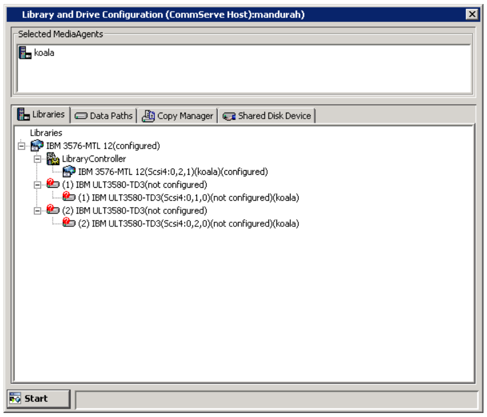
TO REPLACE A CONFIGURED LIBRARY WITH A NEW LIBRARY

1. Deconfigure the drives.

To deconfigure:

From the **Library and Drive Configuration** window, right-click the drive you wish to deconfigure and then click Deconfigure. Click **Yes** in the confirmation prompt that appears.

Note that the drives which were deconfigured appear with the `not configured` status, as shown in the sample image.



```
koala
```

```
Libraries
⊟ IBM 3576-MTL 12(configured)
    ⊟ LibraryController
        IBM 3576-MTL 12(Scsi4:0,2,1)(koala)(configured)
    ⊟ (1) IBM ULT3580-TD3(not configured)
        (1) IBM ULT3580-TD3(Scsi4:0,1,0)(not configured)(koala)
    ⊟ (2) IBM ULT3580-TD3(not configured)
        (2) IBM ULT3580-TD3(Scsi4:0,2,0)(not configured)(koala)
```

WARNING

Do not deconfigure the library, master drive pool or drive pool.

2. Exit the **Library and Drive Configuration** window.

3. Shut down the library and the MediaAgent computer attached to the library.

4. Replace the existing library with the new library.

5. Physically remove the media from the old library and insert them into the new library.

6. Power on the library and reboot the MediaAgent computer.

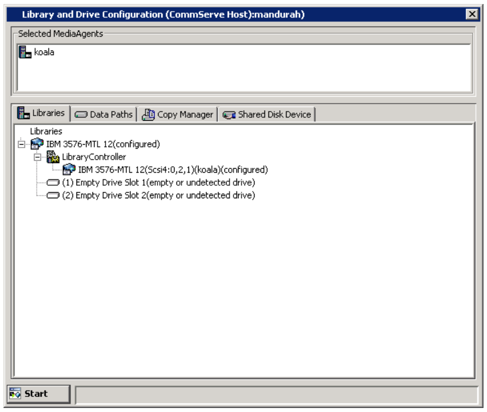
7. Check and verify that the library and drives are visible to the operating system.

For a more detailed explanation on verifying the driver configurations, see Driver Configurations.

8. Display the Library and Drive Configuration window.

Select the MediaAgent attached to the library in the Select MediaAgents dialog box.

Note that the drives in the library are displayed as empty drive slots, as shown in the sample image.



```
koala
```

```
Libraries
⊟ IBM 3576-MTL 12(configured)
    ⊟ LibraryController
        IBM 3576-MTL 12(Scsi4:0,2,1)(koala)(configured)
    (1) Empty Drive Slot 1(empty or undetected drive)
    (2) Empty Drive Slot 2(empty or undetected drive)
```

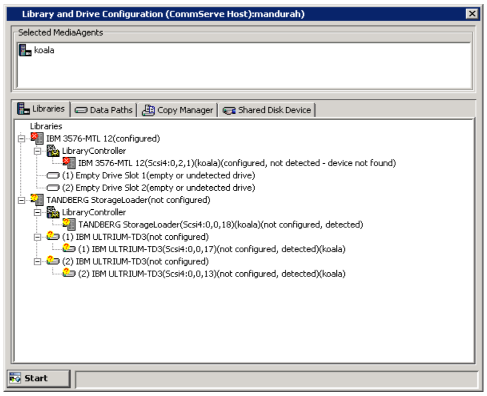
9. Detect the devices as described in Detect Devices.

WARNING

Do not perform the exhaustive detection now.

10. Click **OK** in the error message which indicates that the library could not be detected.

Note that the newly detected library and drives are displayed, as shown in the sample image.



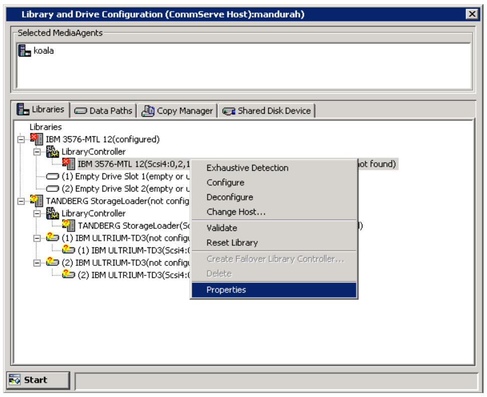
Library and Drive Configuration (CommServe Host):mandurah)

Selected MediaAgents

koala

```
Libraries
IBM 3576-MTL 12(configured)
  LibraryController
    IBM 3576-MTL 12(Scsi4:0,2,1)(koala)(configured, not detected - device not found)
  (1) Empty Drive Slot 1(empty or undetected drive)
  (2) Empty Drive Slot 2(empty or undetected drive)
TANDBERG StorageLoader(not configured)
  LibraryController
    TANDBERG StorageLoader(Scsi4:0,0,18)(koala)(not configured, detected)
  (1) IBM ULTRIUM-TD3(not configured)
    (1) IBM ULTRIUM-TD3(Scsi4:0,0,17)(not configured, detected)(koala)
  (2) IBM ULTRIUM-TD3(not configured)
    (2) IBM ULTRIUM-TD3(Scsi4:0,0,13)(not configured, detected)(koala)
```

11. Right-click the library controller associated with the old library and then select **Properties**.

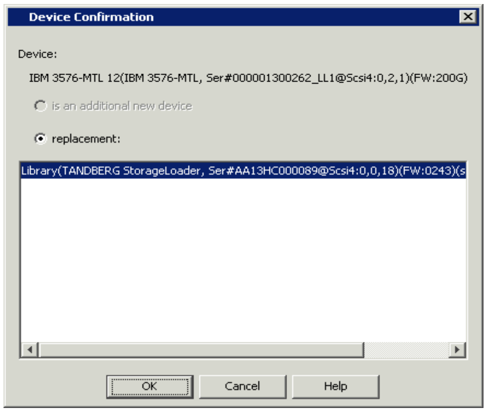


Library and Drive Configuration (CommServe Host):mandurah)

12. From the **Library Controller Properties** window click the **Modify** button.

Note the following in the **Device Confirmation** dialog box:

- The Device information contains the serial number of the old library.
- The serial number for the new library along with other library information is displayed below the **replacement** option.



Device Confirmation

Device:

IBM 3576-MTL 12(IBM 3576-MTL, Ser#000001300262_LL1@Scsi4:0,2,1)(FW:200G)

○ is an additional new device

● replacement:

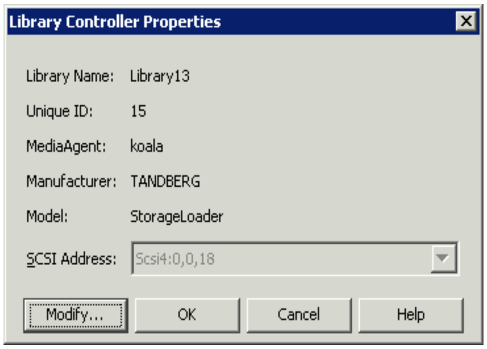
Library(TANDBERG StorageLoader, Ser#AA13HC000089@Scsi4:0,0,18)(FW:0243)(s

13. Click and highlight the new library and then click **OK**.

14. Click **Yes** in the confirmation prompt.

15. The **Library Controller Properties** window gets updated with the SCSI Address of the new library.

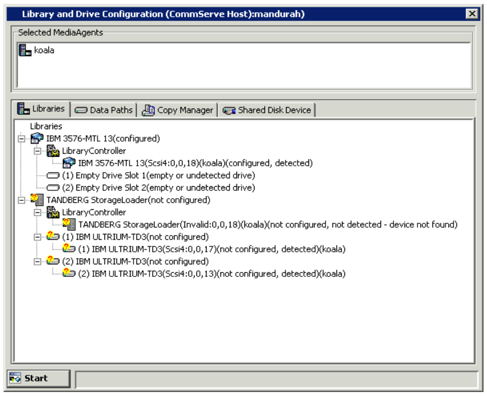
Click **OK**.



Library Controller Properties

Library Name:	Library13
Unique ID:	15
MediaAgent:	koala
Manufacturer:	TANDBERG
Model:	StorageLoader
SCSI Address:	Scsi4:0,0,18

The new library information is displayed, as shown in the sample image.

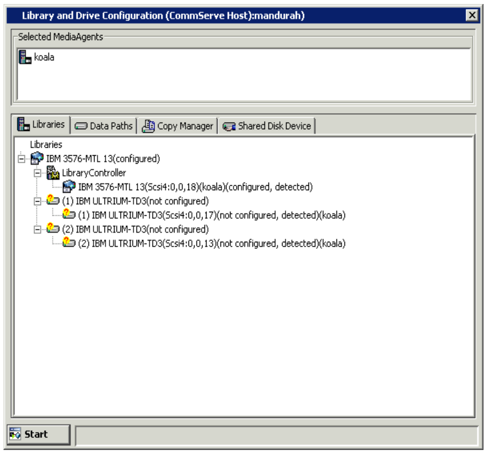


Selected MediaAgents: koala

```
Libraries
IBM 3576-MTL 13(configured)
  LibraryController
    IBM 3576-MTL 13(Scsi4:0,0,18)(koala)(configured, detected)
  (1) Empty Drive Slot 1(empty or undetected drive)
  (2) Empty Drive Slot 2(empty or undetected drive)
TANDBERG StorageLoader(not configured)
  LibraryController
    TANDBERG StorageLoader(Invalid:0,0,18)(koala)(not configured, not detected - device not found)
  (1) IBM ULTRIUM-TD3(not configured)
    (1) IBM ULTRIUM-TD3(Scsi4:0,0,17)(not configured, detected)(koala)
  (2) IBM ULTRIUM-TD3(not configured)
    (2) IBM ULTRIUM-TD3(Scsi4:0,0,13)(not configured, detected)(koala)
```

16. Perform an exhaustive detection of devices as described in Detect Devices Using Exhaustive Detection.

    All the drives will be detected and displayed with a **detected** status in the **Library and Drive Configuration** window, as shown in the sample image.



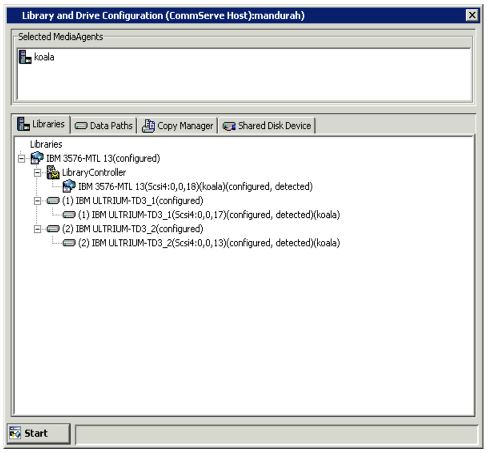
Selected MediaAgents: koala

```
Libraries
IBM 3576-MTL 13(configured)
  LibraryController
    IBM 3576-MTL 13(Scsi4:0,0,18)(koala)(configured, detected)
  (1) IBM ULTRIUM-TD3(not configured)
    (1) IBM ULTRIUM-TD3(Scsi4:0,0,17)(not configured, detected)(koala)
  (2) IBM ULTRIUM-TD3(not configured)
    (2) IBM ULTRIUM-TD3(Scsi4:0,0,13)(not configured, detected)(koala)
```

17. Configure the library as described in Configure Devices.

    In the **Configuration** dialog box, select the **Library and all drives** option, to configure the library.

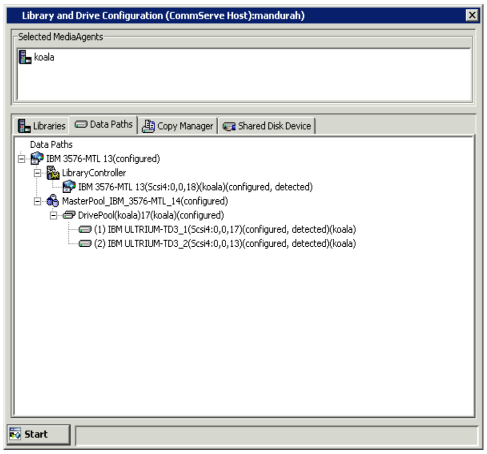
    The **Library** tab provides the physical view of the devices (library and drives).



Selected MediaAgents: koala

```
Libraries
IBM 3576-MTL 13(configured)
  LibraryController
    IBM 3576-MTL 13(Scsi4:0,0,18)(koala)(configured, detected)
  (1) IBM ULTRIUM-TD3_1(configured)
    (1) IBM ULTRIUM-TD3_1(Scsi4:0,0,17)(configured, detected)(koala)
  (2) IBM ULTRIUM-TD3_2(configured)
    (2) IBM ULTRIUM-TD3_2(Scsi4:0,0,13)(configured, detected)(koala)
```

The **Data Paths** tab provides a logical view of the data path used to access the devices - library, master drive pool, drive pool, drive.



Selected MediaAgents: koala

```
Data Paths
IBM 3576-MTL 13(configured)
  LibraryController
    IBM 3576-MTL 13(Scsi4:0,0,18)(koala)(configured, detected)
  MasterPool_IBM_3576-MTL_14(configured)
    DrivePool(koala)17(koala)(configured)
      (1) IBM ULTRIUM-TD3_1(Scsi4:0,0,17)(configured, detected)(koala)
      (2) IBM ULTRIUM-TD3_2(Scsi4:0,0,13)(configured, detected)(koala)
```

Add a Same Drive Type

The following procedure outlines the steps involved in adding a similar drive type to an existing library.

BEFORE YOU BEGIN

- The new drive must be similar to the drive types already available in the library.

TO ADD A DRIVE OF THE SAME DRIVE TYPE

1. Shut down the library and the MediaAgent computer attached to the library and replace the existing drive with the new drive.
2. Power on the library and reboot the MediaAgent computer.
3. Check and verify that the replaced drive is visible to the operating system.

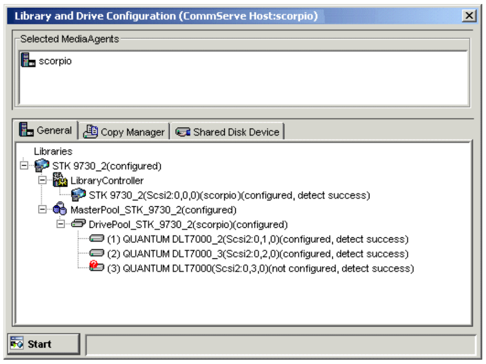
   For a more detailed explanation on verifying the driver configurations, see Driver Configurations.
4. Display the Library and Drive Configuration window.

   Select the MediaAgent attached to the library in the `Select MediaAgents` dialog box.
5. Detect the devices as described in Detect Devices.

   WARNING

   Do not perform the exhaustive detection now.

   The new drive will be displayed with the `not configured, detect success status`.



```
Libraries
STK 9730_2(configured)
  LibraryController
    STK 9730_2(Scsi2:0,0,0)(scorpio)(configured, detect success)
  MasterPool_STK_9730_2(configured)
    DrivePool_STK_9730_2(scorpio)(configured)
      (1) QUANTUM DLT7000_2(Scsi2:0,1,0)(configured, detect success)
      (2) QUANTUM DLT7000_3(Scsi2:0,2,0)(configured, detect success)
      (3) QUANTUM DLT7000(Scsi2:0,3,0)(not configured, detect success)
```

6. Configure the library as described in Configure Devices.

   In the **Device Configuration** dialog box, choose the **Do Exhaustive Detection Now** option.

   The status of the drive changes to `configured`.

Add a Compatible Drive Type

The following procedure outlines the steps involved in adding a compatible drive type to an existing library.

To add a compatible drive type in the library

1. Shut down the library and the MediaAgent computer attached to the library and add the new drive.
2. Power on the library and reboot the MediaAgent computer.
3. Check and verify that the newly added drive is visible to the operating system. For a more detailed explanation on verifying the driver configurations, see Driver Configurations.
4. Display the Library and Drive Configuration window.

   Select the MediaAgent attached to the library in the **Select MediaAgents** dialog box.
5. Detect the devices as described in Detect Devices.

   Do not perform the exhaustive detection now.

   The new drive will be displayed with the not configured, detect success status.
6. Right-click the library with the mixed drive types, and then choose **Add MasterDrivePool**.

   A **Master Drive Pool** is created for the library.

7. Right-click the newly created Master Drive Pool, and then choose **Add DrivePool**.
8. From the **Select MediaAgent** dialog box, select the MediaAgent to which you wish to associate the drive pool and then click **OK**. A **Drive Pool** is created in the Master Drive Pool.
9. Drag and drop the new drives into the new Drive Pool. If you have multiple drives, ensure that all the drives within this drive pool are of the same type.
10. Repeat steps 6 to 9 if you have another drive type in the library.
11. Configure the library as described in Configure Devices.
12. Optionally rename the Master Drive Pools and Drive Pools in the library with appropriate names, to avoid confusion.
13. Create new scratch pools and import the appropriate media into the scratch pool. For a detailed explanation of this step, see Library with Mixed Drive Types - Post Configuration Considerations.

AUTOMATICALLY DETECT REPLACED DRIVES

Required Capability: See Capabilities and Permitted Actions

To automatically detect replaced drives:

1. From the CommCell Browser, right-click the library for which you wish to enable the option to automatically detect replaced drives, and then click **Properties**.
2. Click the Drive tab.
3. From the **Attributes** region, choose **Enable Auto Drive Replacement when new device is detected during Mount** to enable this option. (Clear this check box to disable this option.)
4. Click **OK** to save the changes.

NOTES

- This is recommended method for replacing compatible drives as it provides a one touch solution for replacing drives.
- In some cases the system may not automatically detect the new drives. e.g., if the library does not support drive serialization, if the drive is not replaced with a compatible drive type, if the library is attached to a Solaris MediaAgent, etc. In such cases, use one of the following procedures for replacing drives:
  - Replace a Drive with the Same Drive Type
  - Replace a Drive with the Compatible Drive Type
  - Replace a Drive With the Same Drive Type in the SAN DDS Environment
  - Replace a Drive With a Compatible Drive Type in the SAN DDS Environment

REPLACE A DRIVE WITH THE SAME DRIVE TYPE

The following procedure outlines the steps involved in replacing a drive with the same drive type to an existing library, without deconfiguring the library.

BEFORE YOU BEGIN

- The new drive must be similar to the drive types already available in the library.

TO REPLACE A DRIVE OF THE SAME DRIVE TYPE

1. Shut down the library and the MediaAgent computer attached to the library and replace the existing drive with the new drive.
2. Power on the library and reboot the MediaAgent computer.
3. Check and verify that the replaced drive is visible to the operating system.

   For a more detailed explanation on verifying the driver configurations, see Driver Configurations.
4. Display the Library and Drive Configuration window. Select the MediaAgent attached to the library in the **Select MediaAgents** window.

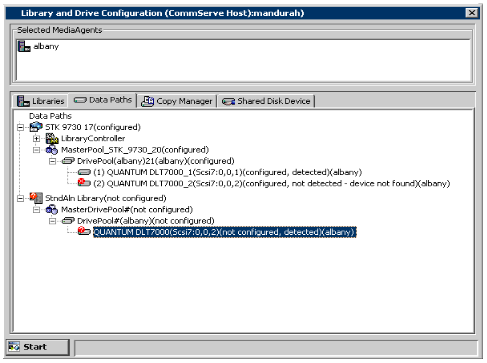
   Follow the steps given below to detect the new drive. Newer drives get detected automatically; verify the new drive in Step 11 below.
5. Detect the devices as described in Detect Devices.

   WARNING

   Do not perform the exhaustive detection now.
6. Click **OK** in the error message which indicates that the library could not be detected.

   The old drive which was removed is displayed with the `not configured, not detect`

`- device not found` status, while the newly detected drive is displayed as a stand alone drive, as shown in the sample image.

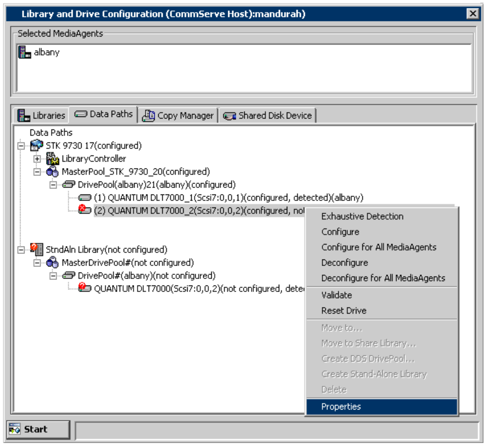


Library and Drive Configuration (CommServe Host):mandurah)

Selected MediaAgents: albany

```
Data Paths
STK 9730 17(configured)
    LibraryController
    MasterPool_STK_9730_20(configured)
        DrivePool(albany)21(albany)(configured)
            (1) QUANTUM DLT7000_1(Scsi7:0,0,1)(configured, detected)(albany)
            (2) QUANTUM DLT7000_2(Scsi7:0,0,2)(configured, not detected - device not found)(albany)
StndAln Library(not configured)
    MasterDrivePool#(not configured)
        DrivePool#(albany)(not configured)
            QUANTUM DLT7000(Scsi7:0,0,2)(not configured, detected)(albany)
```

7. Right-click the library controller associated with the old library and then select **Properties**.



Library and Drive Configuration (CommServe Host):mandurah)

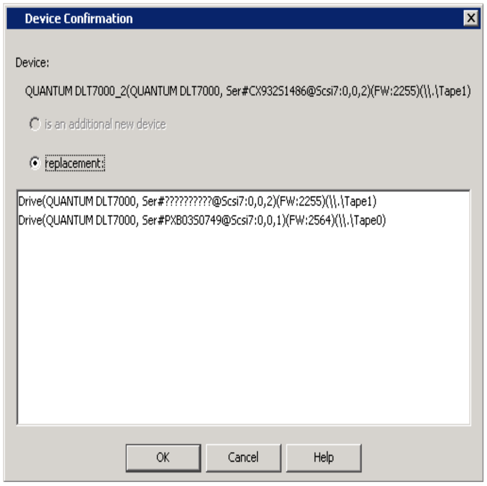
Selected MediaAgents: albany

```
Data Paths
STK 9730 17(configured)
    LibraryController
    MasterPool_STK_9730_20(configured)
        DrivePool(albany)21(albany)(configured)
            (1) QUANTUM DLT7000_1(Scsi7:0,0,1)(configured, detected)(albany)
            (2) QUANTUM DLT7000_2(Scsi7:0,0,2)(configured, no
StndAln Library(not configured)
    MasterDrivePool#(not configured)
        DrivePool#(albany)(not configured)
            QUANTUM DLT7000(Scsi7:0,0,2)(not configured, dete
```

8. From the **Drive Properties** window click the **Modify** button.

Note the following in the **Device Confirmation** window:

- The **Device** information contains the serial number of the old drive.
- The serial number for all the drives available in the library are displayed below the **is the following device** option.



Device Confirmation

Device:

QUANTUM DLT7000_2(QUANTUM DLT7000, Ser#CX93251486@Scsi7:0,0,2)(FW:2255)(\\.\Tape1)

○ is an additional new device

● replacement:

```
Drive(QUANTUM DLT7000, Ser#??????????@Scsi7:0,0,2)(FW:2255)(\\.\Tape1)
Drive(QUANTUM DLT7000, Ser#PXB0350749@Scsi7:0,0,1)(FW:2564)(\\.\Tape0)
```

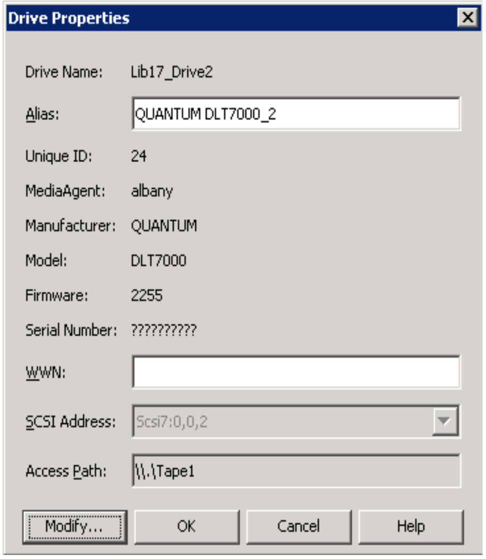
9. Click and highlight the new drive and then click **OK**.

NOTES

Verify and ensure that you select the appropriate serial number associated with the newly replaced drive.

10. Click **OK** in the confirmation prompt.

The **Drive Properties** window box gets updated with the Serial Number and SCSI Address of the new drive.



Drive Properties

Drive Name: Lib17_Drive2

Alias: QUANTUM DLT7000_2

Unique ID: 24

MediaAgent: albany

Manufacturer: QUANTUM

Model: DLT7000

Firmware: 2255

Serial Number: ??????????

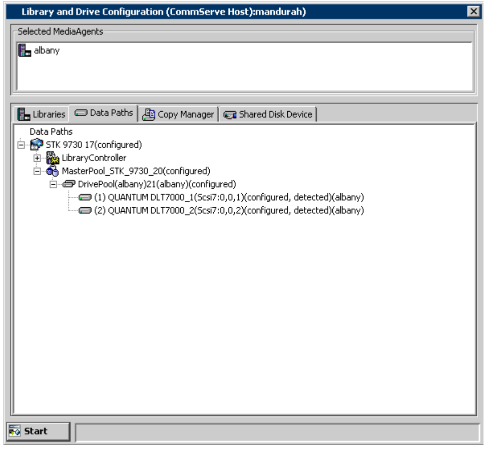
WWN:

SCSI Address: Scsi7:0,0,2

Access Path: \\.\Tape1

11. Click **OK**.

The new drive is replaced in the **Library and Drive Configuration** window, as shown in the sample image.



Library and Drive Configuration (CommServe Host):mandurah)

Selected MediaAgents: albany

```
Data Paths
STK 9730 17(configured)
    LibraryController
    MasterPool_STK_9730_20(configured)
        DrivePool(albany)21(albany)(configured)
            (1) QUANTUM DLT7000_1(Scsi7:0,0,1)(configured, detected)(albany)
            (2) QUANTUM DLT7000_2(Scsi7:0,0,2)(configured, detected)(albany)
```

12. Perform an exhaustive detection of devices as described in Detect Devices Using Exhaustive Detection.

REPLACE A DRIVE WITH THE COMPATIBLE DRIVE TYPE

The following procedure outlines the steps involved in replacing a drive with a compatible drive type to an existing library, without deconfiguring the library.

BEFORE YOU BEGIN

The following process creates a new drive pool for the drive(s) that are replaced with a compatible drive type.
As the number of configured drives in a drive pool cannot be smaller than the largest number of streams used by any storage policy that accesses that drive pool, verify and if necessary reduce the number of streams in storage policy copies to be equal to the number of functional drives in the drive pool.

For example, assume that a drive pool containing four drives is accessed by a four stream storage policy. If you wish to replace one of the drives with a compatible drive type, you must first reduce the four-streamed storage policies to three-streams.

WARNING

Previous database backups using multiple streams cannot be restored if the number of streams in a storage policy is reduced.

TO REPLACE A DRIVE OF THE SAME DRIVE TYPE

1. Deconfigure the drive that want to replace.

To deconfigure:

From the **Library and Drive Configuration** window, right-click the drive you wish to deconfigure and then click **Deconfigure**.

Click **Yes** in the confirmation prompt that appears.

2. Shut down the library and the MediaAgent computer attached to the library and replace the existing drive with the new drive.

3. Power on the library and reboot the MediaAgent computer.

4. Check and verify that the replaced drive is visible to the operating system.

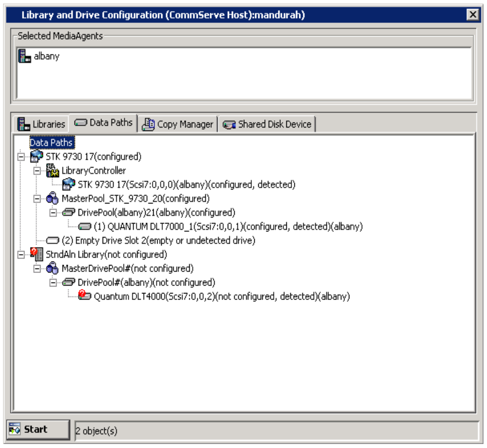
For a more detailed explanation on verifying the driver configurations, see Driver Configurations.

5. Display the Library and Drive Configuration window.

Select the MediaAgent attached to the library in the **Select MediaAgents** dialog box.

6. Detect the devices as described in Detect Devices.

Note that the new drive(s) will be displayed as a **StndAln** library with the **not configured, detect success** status, as shown in the sample image. The **Master Drive Pool** and **Drive Pool** are automatically added.

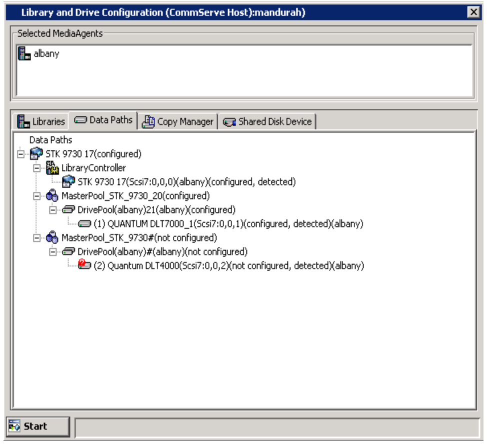


```
Data Paths
STK 9730 17(configured)
  LibraryController
    STK 9730 17(Scsi7:0,0,0)(albany)(configured, detected)
  MasterPool_STK_9730_20(configured)
    DrivePool(albany)21(albany)(configured)
      (1) QUANTUM DLT7000_1(Scsi7:0,0,1)(configured, detected)(albany)
  (2) Empty Drive Slot 2(empty or undetected drive)
StndAln Library(not configured)
  MasterDrivePool#(not configured)
    DrivePool#(albany)(not configured)
      Quantum DLT4000(Scsi7:0,0,2)(not configured, detected)(albany)
```

WARNING

Do not perform the exhaustive detection now.

7. Drag the newly created **Master Drive Pool** from the **StndAln** library and drop it into the previously configured library (In the example, **STK 9730 17**).



```
Data Paths
STK 9730 17(configured)
  LibraryController
    STK 9730 17(Scsi7:0,0,0)(albany)(configured, detected)
  MasterPool_STK_9730_20(configured)
    DrivePool(albany)21(albany)(configured)
      (1) QUANTUM DLT7000_1(Scsi7:0,0,1)(configured, detected)(albany)
  MasterPool_STK_9730#(not configured)
    DrivePool(albany)#(albany)(not configured)
      (2) Quantum DLT4000(Scsi7:0,0,2)(not configured, detected)(albany)
```

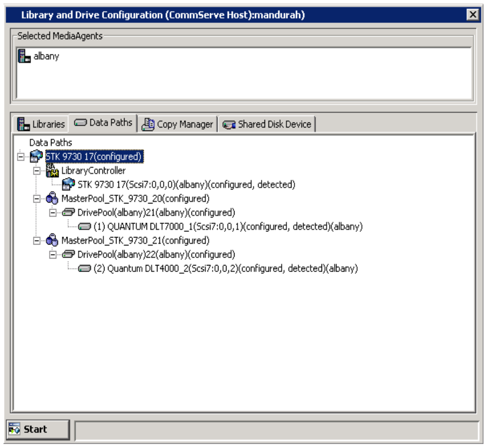
8. Repeat the previous step if you are replacing more than one drive in the library.

9. Configure the master drive pool.

To Configure:

Right-click the master drive pool you wish to configure and then click **Configure**.

Click **Master drive pool and all drives** in the **Configuration** prompt that appears.



```
Data Paths
STK 9730 17(configured)
  LibraryController
    STK 9730 17(Scsi7:0,0,0)(albany)(configured, detected)
  MasterPool_STK_9730_20(configured)
    DrivePool(albany)21(albany)(configured)
      (1) QUANTUM DLT7000_1(Scsi7:0,0,1)(configured, detected)(albany)
  MasterPool_STK_9730_21(configured)
    DrivePool(albany)22(albany)(configured)
      (2) Quantum DLT4000_2(Scsi7:0,0,2)(configured, detected)(albany)
```

10. Optionally rename the Master Drive Pools and Drive Pools in the library with appropriate names, to avoid confusion.

11. Create new scratch pools and import the appropriate media into the scratch pool. Re-associate some of the storage policy copies with the new scratch pool. For a detailed explanation of this step, see Configure a Direct-Attached Library with Mixed Drive Types.

Replace a Library in the SAN DDS Environment

The following procedure outlines the steps involved in replacing an existing library with a new library without deconfiguring the existing library in a SAN DDS environment.

Before you Begin

- The new library should have the same drive type
- The number of drives in the new library must be the same or more

To replace a configured library with a new library in a SAN DDS environment

1. Deconfigure the drives only.

   From the **Library and Drive Configuration** window, right-click the drive you wish to deconfigure and then click **Deconfigure**.

   Click **Yes** in the confirmation prompt that appears.
2. Deconfigure all the fail over library controllers, except one.

   Do not deconfigure the library, master drive pool or drive pool.
3. Exit the **Library and Drive Configuration** window.
4. Shut down all the devices (library, routers and switches) and the MediaAgent computers attached to the library.
5. Replace the existing library with the new library.
6. Physically remove the media from the old library and insert them into the new library.
7. Power on the library and reboot all the MediaAgent computers and any other devices that may apply (e.g. routers and switches in a SAN environment.)
8. Check and verify that the library and drives are visible to the operating system.

   For a more detailed explanation on verifying the driver configurations, see the Driver Configurations.
9. Display the Library and Drive Configuration window.

   Select the MediaAgent that has the configured library controller, in the **Select MediaAgents** windows.

   The drives in the new library are displayed as empty drive slots, in the **Library and Drive Configuration** window.
10. Detect the devices that are controlled by MediaAgents that will access the library as described in Detect Devices.

    Do not perform the exhaustive detection now.
11. Click OK in the prompt with the message **Cannot detect library.....**

    The new library with the drives are displayed with the `not configured` status in the **Library and Drive Configuration** window.
12. Right-click the library controller associated with the old library and then select **Properties**.
13. From the **Library Controller Properties** windows click the **Modify** button.

    Note the following in the **Device Confirmation** windows:

    - The **Device** information contains the serial number of the old library
    - The serial number for the new library along with other library information is displayed below the **is the following** device option.
14. Click and highlight the new library and then click **OK**.

    Click **OK** in the confirmation prompt.

    The **Library Controller Properties** window gets updated with the **SCSI Address** of the new library.

    Click **OK**.
15. Configure the drives in the MediaAgent.
16. From the **Library and Drive Configuration** window, click the **Start** menu and choose **Select MediaAgents**.

    From the **Select MediaAgents** window, select *all* the MediaAgents that share the library.
17. Detect the devices that are controlled by MediaAgents that will access the library as described in Detect Devices.

    Make sure that the **Automatically create DDS Drivepools** option is selected in the **Detect Library** window.
18. Click **OK** in the Information prompt that appears.

    The system detects the library and drives and automatically displays them with the DDS setup in the **Library and Drive Configuration** window.

19. Configure the library as described in Configure Devices.

    In the **Configuration** window, select the **Library and all drives** option to configure the library.

ADD A SAME DRIVE TYPE IN THE SAN DDS ENVIRONMENT

The following procedure outlines the steps involved in adding a similar drive type to an existing library in the SAN DDS environment.

BEFORE YOU BEGIN

- The new drive must be similar to the drive types already available in the library.

TO ADD A DRIVE OF THE SAME DRIVE TYPE IN THE SAN DDS ENVIRONMENT

1. Shut down the library and the MediaAgent computer attached to the library and replace the existing drive with the new drive.

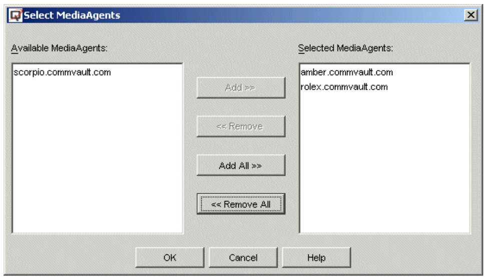
2. Power on the library and reboot the MediaAgent computer.

3. Check and verify that the replaced drive is visible to the operating system.

   For a more detailed explanation on verifying the driver configurations, see Driver Configurations.

4. Display the Library and Drive Configuration window.

   Select all the MediaAgents that share the library in the **Select MediaAgents** dialog box.



Select MediaAgents

Available MediaAgents:
scorpio.commvault.com

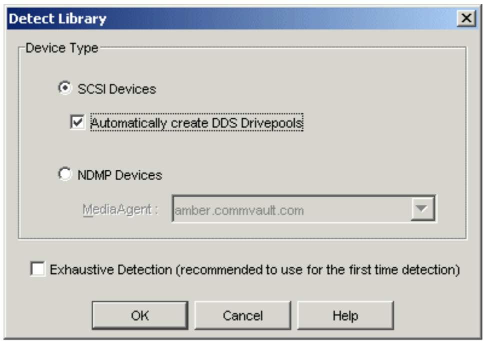
Selected MediaAgents:
amber.commvault.com
rolex.commvault.com

5. Detect the devices as described in Detect Devices.

   WARNING

   Do not perform the exhaustive detection now.

   Make sure that the **Automatically create DDS Drivepools** option is selected in the **Detect Library** dialog box.



Detect Library

Device Type

● SCSI Devices

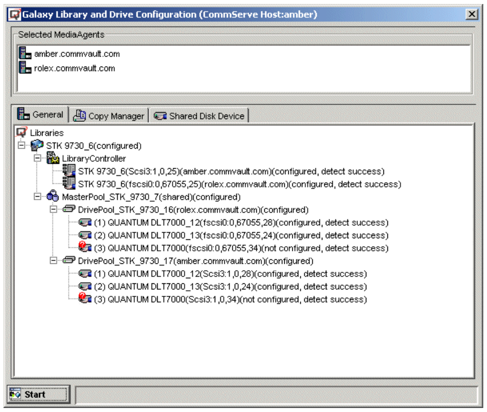
☑ Automatically create DDS Drivepools

○ NDMP Devices

MediaAgent : amber.commvault.com

☐ Exhaustive Detection (recommended to use for the first time detection)

   The system detects the drives and automatically displays them with the DDS setup in the **Library and Drive Configuration** window.

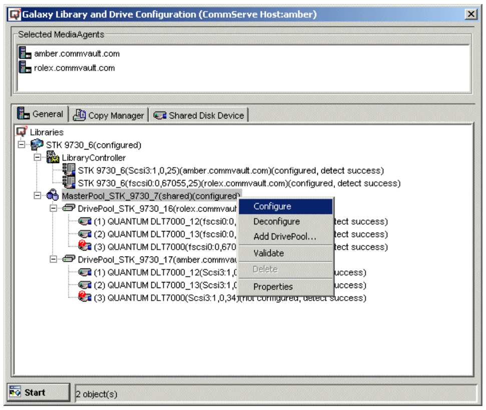


Galaxy Library and Drive Configuration (CommServe Host:amber)

Selected MediaAgents
amber.commvault.com
rolex.commvault.com

```
Libraries
⊟ STK 9730_6(configured)
   ⊟ LibraryController
      STK 9730_6(Scsi3:1,0,25)(amber.commvault.com)(configured, detect success)
      STK 9730_6(fscsi0:0,67055,25)(rolex.commvault.com)(configured, detect success)
   ⊟ MasterPool_STK_9730_7(shared)(configured)
      ⊟ DrivePool_STK_9730_16(rolex.commvault.com)(configured)
         (1) QUANTUM DLT7000_12(fscsi0:0,67055,28)(configured, detect success)
         (2) QUANTUM DLT7000_13(fscsi0:0,67055,24)(configured, detect success)
         (3) QUANTUM DLT7000(fscsi0:0,67055,34)(not configured, detect success)
      ⊟ DrivePool_STK_9730_17(amber.commvault.com)(configured)
         (1) QUANTUM DLT7000_12(Scsi3:1,0,28)(configured, detect success)
         (2) QUANTUM DLT7000_13(Scsi3:1,0,24)(configured, detect success)
         (3) QUANTUM DLT7000(Scsi3:1,0,34)(not configured, detect success)
```

6. Right -click the master drive pool and then select **Configure**.



Galaxy Library and Drive Configuration (CommServe Host:amber)

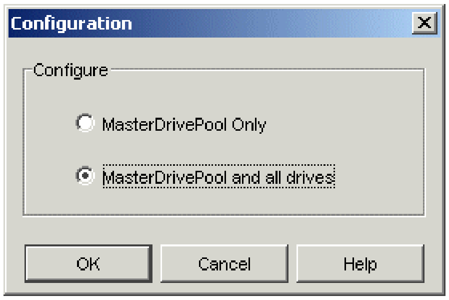
Selected MediaAgents

amber.commvault.com
rolex.commvault.com

Libraries
STK 9730_6(configured)
LibraryController
STK 9730_6(Scsi3:1,0,25)(amber.commvault.com)(configured, detect success)
STK 9730_6(fscsi0:0,67055,25)(rolex.commvault.com)(configured, detect success)
MasterPool_STK_9730_7(shared)(configured)
DrivePool_STK_9730_16(rolex.commvault
(1) QUANTUM DLT7000_12(fscsi0:0, tect success)
(2) QUANTUM DLT7000_13(fscsi0:0, tect success)
(3) QUANTUM DLT7000(fscsi0:0,670 tect success)
DrivePool_STK_9730_17(amber.commvau
(1) QUANTUM DLT7000_12(Scsi3:1,(uccess)
(2) QUANTUM DLT7000_13(Scsi3:1,(uccess)
(3) QUANTUM DLT7000(Scsi3:1,0,34)(not configured, detect success)

2 object(s)

7. In the **Configuration** dialog box, choose the **MasterDrivePool** and **all drive** option.



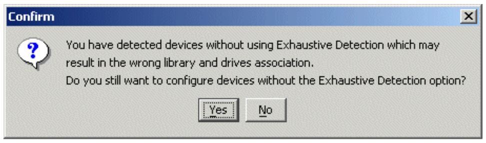
Configuration

Configure

○ MasterDrivePool Only

● MasterDrivePool and all drives

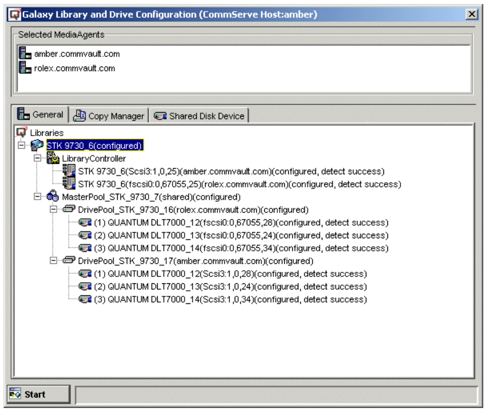
8. Click **OK** in the **Confirm** prompt asking you whether you would like to configure the devices without exhaustive detection.



Confirm

You have detected devices without using Exhaustive Detection which may result in the wrong library and drives association.
Do you still want to configure devices without the Exhaustive Detection option?

The new drive will be displayed with the `configured` status.



Galaxy Library and Drive Configuration (CommServe Host:amber)

Selected MediaAgents

amber.commvault.com
rolex.commvault.com

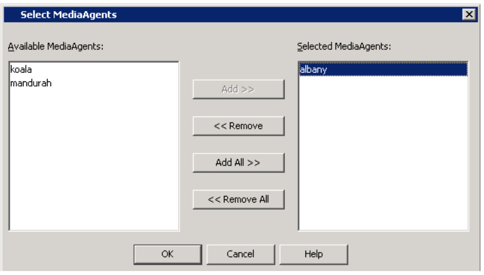
Libraries
STK 9730_6(configured)
LibraryController
STK 9730_6(Scsi3:1,0,25)(amber.commvault.com)(configured, detect success)
STK 9730_6(fscsi0:0,67055,25)(rolex.commvault.com)(configured, detect success)
MasterPool_STK_9730_7(shared)(configured)
DrivePool_STK_9730_16(rolex.commvault.com)(configured)
(1) QUANTUM DLT7000_12(fscsi0:0,67055,28)(configured, detect success)
(2) QUANTUM DLT7000_13(fscsi0:0,67055,24)(configured, detect success)
(3) QUANTUM DLT7000_14(fscsi0:0,67055,34)(configured, detect success)
DrivePool_STK_9730_17(amber.commvault.com)(configured)
(1) QUANTUM DLT7000_12(Scsi3:1,0,28)(configured, detect success)
(2) QUANTUM DLT7000_13(Scsi3:1,0,24)(configured, detect success)
(3) QUANTUM DLT7000_14(Scsi3:1,0,34)(configured, detect success)

ADD A COMPATIBLE DRIVE TYPE IN THE SAN DDS ENVIRONMENT

The following procedure outlines the steps involved in adding a compatible drive type to an existing library in the SAN environment, without deconfiguring the library.

TO ADD A COMPATIBLE DRIVE TYPE IN THE SAN DDS ENVIRONMENT

1. Shut down the library and the MediaAgent computer attached to the library and replace the existing drive with the new drive.
2. Power on the library and reboot the MediaAgent computer.
3. Check and verify that the replaced drive is visible to the operating system. For a more detailed explanation on verifying the driver configurations, see Driver Configurations.
4. Display the Library and Drive Configuration window.
5. In the **Select MediaAgents** dialog box, select any *one* of the MediaAgents that share the library.



Select MediaAgents

Available MediaAgents:

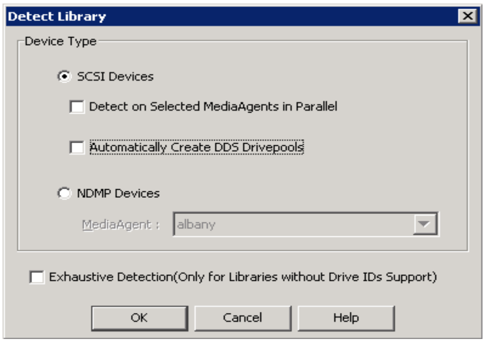
koala
mandurah

Selected MediaAgents:

albany

6. Detect the devices as described in Detect Devices.

   Do not select the **Automatically create DDS Drivepools** option in the **Detect Library** dialog box.



Detect Library

Device Type

● SCSI Devices

□ Detect on Selected MediaAgents in Parallel

□ Automatically Create DDS Drivepools

○ NDMP Devices

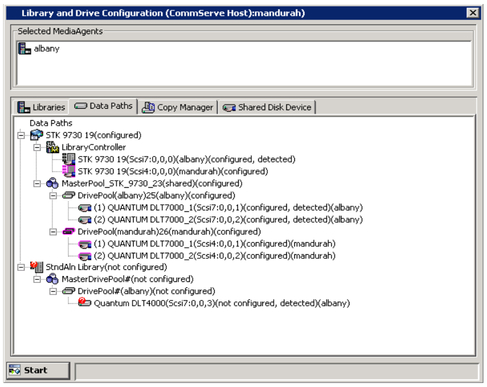
MediaAgent : albany

□ Exhaustive Detection(Only for Libraries without Drive IDs Support)

WARNING

Do not perform the exhaustive detection now.

The new drive will be displayed as a **StndAln** library with the `not configured` status. The **Master Drive Pool** and **Drive Pool** are automatically added.



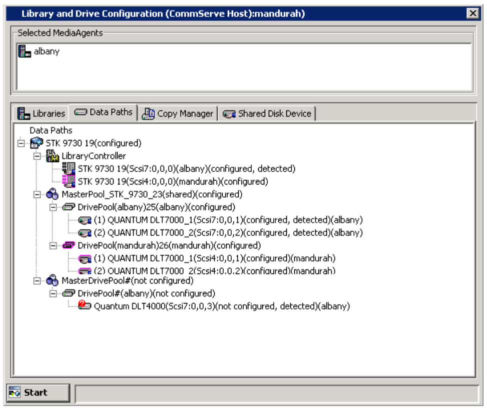
Library and Drive Configuration (CommServe Host):mandurah)

Selected MediaAgents

albany

```
Data Paths
STK 9730 19(configured)
  LibraryController
    STK 9730 19(Scsi7:0,0,0)(albany)(configured, detected)
    STK 9730 19(Scsi4:0,0,0)(mandurah)(configured)
  MasterPool_STK_9730_23(shared)(configured)
    DrivePool(albany)25(albany)(configured)
      (1) QUANTUM DLT7000_1(Scsi7:0,0,1)(configured, detected)(albany)
      (2) QUANTUM DLT7000_2(Scsi7:0,0,2)(configured, detected)(albany)
    DrivePool(mandurah)26(mandurah)(configured)
      (1) QUANTUM DLT7000_1(Scsi4:0,0,1)(configured)(mandurah)
      (2) QUANTUM DLT7000_2(Scsi4:0,0,2)(configured)(mandurah)
StndAln Library(not configured)
  MasterDrivePool#(not configured)
    DrivePool#(albany)(not configured)
      Quantum DLT4000(Scsi7:0,0,3)(not configured, detected)(albany)
```

7. Drag the newly created **Master Drive Pool** from the **StndAln** library and drop it into the previously configured library (In the example, **STK 9730 19**).



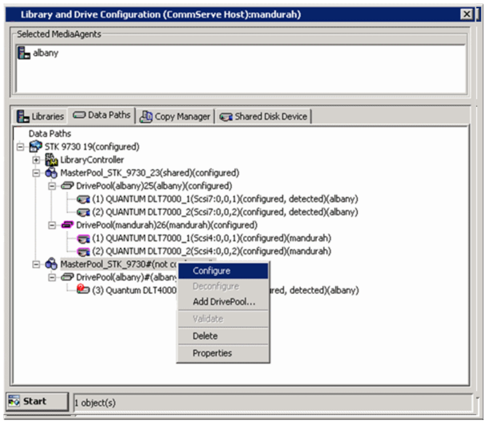
Library and Drive Configuration (CommServe Host):mandurah)

Selected MediaAgents

albany

```
Data Paths
STK 9730 19(configured)
  LibraryController
    STK 9730 19(Scsi7:0,0,0)(albany)(configured, detected)
    STK 9730 19(Scsi4:0,0,0)(mandurah)(configured)
  MasterPool_STK_9730_23(shared)(configured)
    DrivePool(albany)25(albany)(configured)
      (1) QUANTUM DLT7000_1(Scsi7:0,0,1)(configured, detected)(albany)
      (2) QUANTUM DLT7000_2(Scsi7:0,0,2)(configured, detected)(albany)
    DrivePool(mandurah)26(mandurah)(configured)
      (1) QUANTUM DLT7000_1(Scsi4:0,0,1)(configured)(mandurah)
      (2) QUANTUM DLT7000_2(Scsi4:0,0,2)(configured)(mandurah)
  MasterDrivePool#(not configured)
    DrivePool#(albany)(not configured)
      Quantum DLT4000(Scsi7:0,0,3)(not configured, detected)(albany)
```

8. Configure the master drive pool as described in Configure the Master Drive Pool.



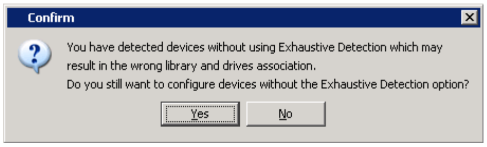
Library and Drive Configuration (CommServe Host):mandurah)

Selected MediaAgents: albany

```
Data Paths
⊟ STK 9730 19(configured)
   ⊞ LibraryController
   ⊟ MasterPool_STK_9730_23(shared)(configured)
      ⊟ DrivePool(albany)25(albany)(configured)
           (1) QUANTUM DLT7000_1(Scsi7:0,0,1)(configured, detected)(albany)
           (2) QUANTUM DLT7000_2(Scsi7:0,0,2)(configured, detected)(albany)
      ⊟ DrivePool(mandurah)26(mandurah)(configured)
           (1) QUANTUM DLT7000_1(Scsi4:0,0,1)(configured)(mandurah)
           (2) QUANTUM DLT7000_2(Scsi4:0,0,2)(configured)(mandurah)
   ⊟ MasterPool_STK_9730#(not co
      ⊟ DrivePool(albany)#(albany
           (3) Quantum DLT4000          red, detected)(albany)
```

1 object(s)

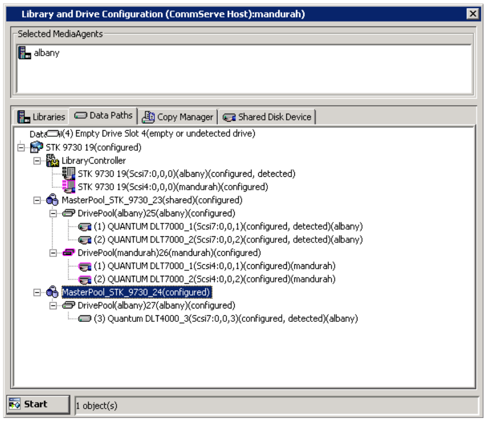
9. Click **OK** in the **Confirm** prompt asking you whether you would like to configure the devices without exhaustive detection.



Confirm

You have detected devices without using Exhaustive Detection which may result in the wrong library and drives association.
Do you still want to configure devices without the Exhaustive Detection option?

10. The master drive pool, with the new drive is configured for the MediaAgent.



Library and Drive Configuration (CommServe Host):mandurah)

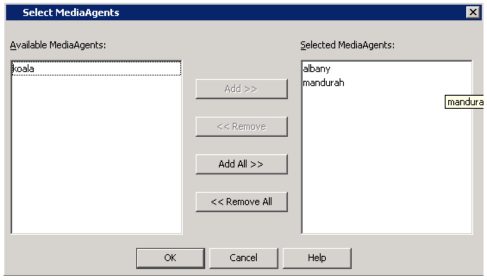
Selected MediaAgents: albany

```
Data(4) Empty Drive Slot 4(empty or undetected drive)
⊟ STK 9730 19(configured)
   ⊟ LibraryController
        STK 9730 19(Scsi7:0,0,0)(albany)(configured, detected)
        STK 9730 19(Scsi4:0,0,0)(mandurah)(configured)
   ⊟ MasterPool_STK_9730_23(shared)(configured)
      ⊟ DrivePool(albany)25(albany)(configured)
           (1) QUANTUM DLT7000_1(Scsi7:0,0,1)(configured, detected)(albany)
           (2) QUANTUM DLT7000_2(Scsi7:0,0,2)(configured, detected)(albany)
      ⊟ DrivePool(mandurah)26(mandurah)(configured)
           (1) QUANTUM DLT7000_1(Scsi4:0,0,1)(configured)(mandurah)
           (2) QUANTUM DLT7000_2(Scsi4:0,0,2)(configured)(mandurah)
   ⊟ MasterPool_STK_9730_24(configured)
      ⊟ DrivePool(albany)27(albany)(configured)
           (3) Quantum DLT4000_3(Scsi7:0,0,3)(configured, detected)(albany)
```

1 object(s)

11. From the **Library and Drive Configuration** window, click the **Start** menu and choose **Select MediaAgents**.

From the **Select MediaAgents** dialog box, select *all* the MediaAgents that share the library.



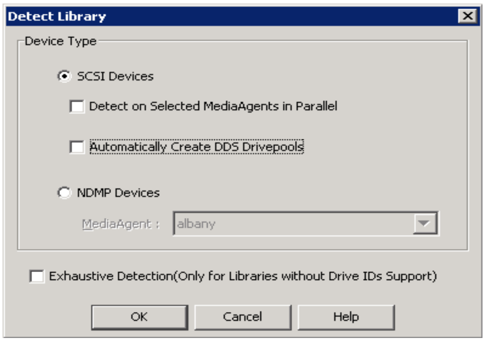
Select MediaAgents

Available MediaAgents: koala

Selected MediaAgents: albany, mandurah

12. Detect the devices that are controlled by MediaAgents that will access the library as described in Detect Devices.

Make sure that the **Automatically create DDS Drivepools** option is selected in the **Detect Library** dialog box.



Detect Library

Device Type

● SCSI Devices

□ Detect on Selected MediaAgents in Parallel

□ Automatically Create DDS Drivepools

○ NDMP Devices

MediaAgent : albany

□ Exhaustive Detection(Only for Libraries without Drive IDs Support)

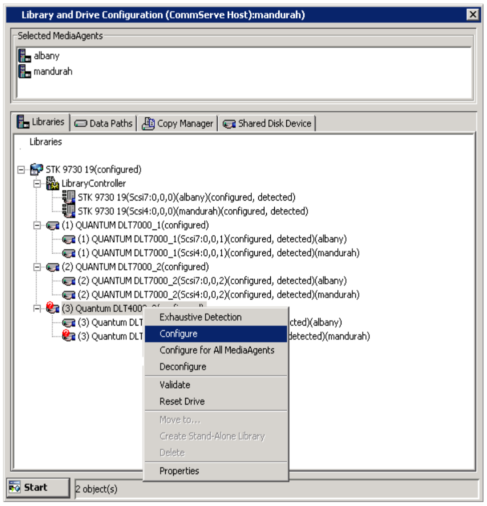
WARNING

Do not perform the exhaustive detection now.

13. Click **OK** in the **Information** prompt that appears.

The system detects the drives and automatically displays them with the DDS setup in the **Library and Drive Configuration** window.

14. Configure the master drive pool, as described in Configure the Master Drive Pool.



Library and Drive Configuration (CommServe Host):mandurah)

Selected MediaAgents

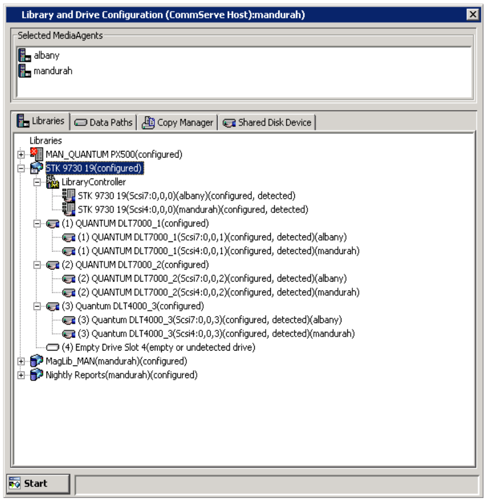
albany
mandurah

Libraries

STK 9730 19(configured)
LibraryController
STK 9730 19(Scsi7:0,0,0)(albany)(configured, detected)
STK 9730 19(Scsi4:0,0,0)(mandurah)(configured, detected)
(1) QUANTUM DLT7000_1(configured)
(1) QUANTUM DLT7000_1(Scsi7:0,0,1)(configured, detected)(albany)
(1) QUANTUM DLT7000_1(Scsi4:0,0,1)(configured, detected)(mandurah)
(2) QUANTUM DLT7000_2(configured)
(2) QUANTUM DLT7000_2(Scsi7:0,0,2)(configured, detected)(albany)
(2) QUANTUM DLT7000_2(Scsi4:0,0,2)(configured, detected)(mandurah)
(3) Quantum DLT400
(3) Quantum DLT cted)(albany)
(3) Quantum DLT detected)(mandurah)

2 object(s)

The master drive pool is configured for the library with the new drive.



Library and Drive Configuration (CommServe Host):mandurah)

Selected MediaAgents

albany
mandurah

Libraries
MAN_QUANTUM PX500(configured)
STK 9730 19(configured)
LibraryController
STK 9730 19(Scsi7:0,0,0)(albany)(configured, detected)
STK 9730 19(Scsi4:0,0,0)(mandurah)(configured, detected)
(1) QUANTUM DLT7000_1(configured)
(1) QUANTUM DLT7000_1(Scsi7:0,0,1)(configured, detected)(albany)
(1) QUANTUM DLT7000_1(Scsi4:0,0,1)(configured, detected)(mandurah)
(2) QUANTUM DLT7000_2(configured)
(2) QUANTUM DLT7000_2(Scsi7:0,0,2)(configured, detected)(albany)
(2) QUANTUM DLT7000_2(Scsi4:0,0,2)(configured, detected)(mandurah)
(3) Quantum DLT4000_3(configured)
(3) Quantum DLT4000_3(Scsi7:0,0,3)(configured, detected)(albany)
(3) Quantum DLT4000_3(Scsi4:0,0,3)(configured, detected)(mandurah)
(4) Empty Drive Slot 4(empty or undetected drive)
MagLib_MAN(mandurah)(configured)
Nightly Reports(mandurah)(configured)

15. Optionally rename the Master Drive Pools and Drive Pools in the library with appropriate names, to avoid confusion.

16. Create new scratch pools and import the appropriate media into the scratch pool. Re-associate some of the storage policy copies with the new scratch pool. For a detailed explanation of this step, see Library with Mixed Drive Types - Post Configuration Considerations.

REPLACE A DRIVE WITH THE SAME DRIVE TYPE IN THE SAN DDS ENVIRONMENT

The following procedure outlines the steps involved in replacing a drive with the same drive type to an existing library, without deconfiguring the library in the SAN DDS environment.

BEFORE YOU BEGIN

- The new drive must be similar to the drive types already available in the library.

TO REPLACE A DRIVE WITH THE SAME DRIVE TYPE IN THE SAN DDS ENVIRONMENT

1. Shut down the library and the MediaAgent computer attached to the library and replace the existing drive with the new drive.

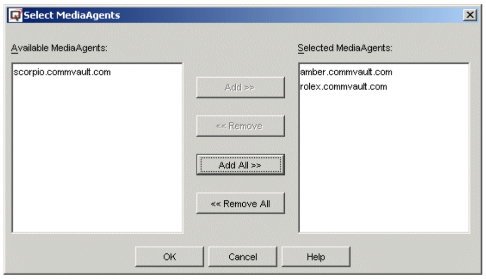
2. Power on the library and reboot the MediaAgent computer.

3. Check and verify that the replaced drive is visible to the operating system.

For a more detailed explanation on verifying the driver configurations, see Driver Configurations.

4. Display the Library and Drive Configuration window.

Select *all* the MediaAgents that share the library in the **Select MediaAgents** window.



Available MediaAgents:
scorpio.commvault.com

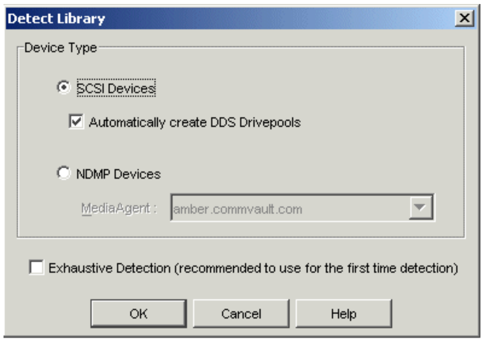
Selected MediaAgents:
amber.commvault.com
rolex.commvault.com

5. Detect the devices as described in Detect Devices.

WARNING

Do not perform the exhaustive detection now.

Make sure that the **Automatically create DDS Drivepools** option is selected in the **Detect Library** window.



● SCSI Devices

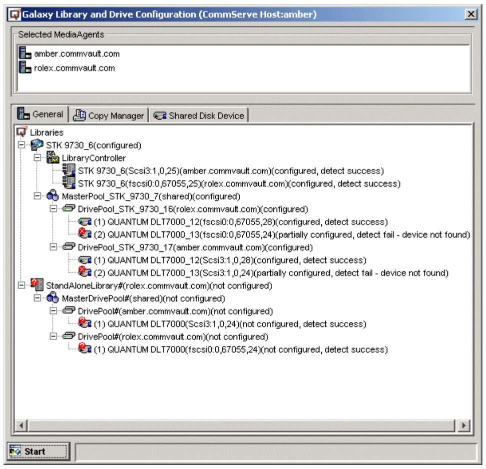
☑ Automatically create DDS Drivepools

○ NDMP Devices

MediaAgent : amber.commvault.com

□ Exhaustive Detection (recommended to use for the first time detection)

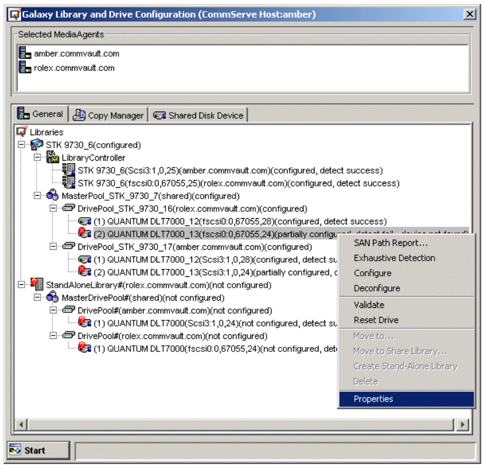
The new drives will be displayed either as a stand-alone drive, if the library controllers are configured, or as a new library for all the MediaAgents sharing the library.


Galaxy Library and Drive Configuration (CommServe Host:amber)
General
Copy Manager
Shared Disk Device
Start

Selected MediaAgents
amber.commvault.com
rolex.commvault.com

```
Libraries
  STK 9730_6(configured)
    LibraryController
      STK 9730_6(Scsi3:1,0,25)(amber.commvault.com)(configured, detect success)
      STK 9730_6(fscsi0:0,67055,25)(rolex.commvault.com)(configured, detect success)
    MasterPool_STK_9730_7(shared)(configured)
      DrivePool_STK_9730_16(rolex.commvault.com)(configured)
        (1) QUANTUM DLT7000_12(fscsi0:0,67055,28)(configured, detect success)
        (2) QUANTUM DLT7000_13(fscsi0:0,67055,24)(partially configured, detect fail - device not found)
      DrivePool_STK_9730_17(amber.commvault.com)(configured)
        (1) QUANTUM DLT7000_12(Scsi3:1,0,28)(configured, detect success)
        (2) QUANTUM DLT7000_13(Scsi3:1,0,24)(partially configured, detect fail - device not found)
  StandAloneLibrary#(rolex.commvault.com)(not configured)
    MasterDrivePool#(shared)(not configured)
      DrivePool#(amber.commvault.com)(not configured)
        (1) QUANTUM DLT7000(Scsi3:1,0,24)(not configured, detect success)
      DrivePool#(rolex.commvault.com)(not configured)
        (1) QUANTUM DLT7000(fscsi0:0,67055,24)(not configured, detect success)
```

6. Right-click the drive that you wish to replace and then select **Properties**.



Selected MediaAgents
amber.commvault.com
rolex.commvault.com

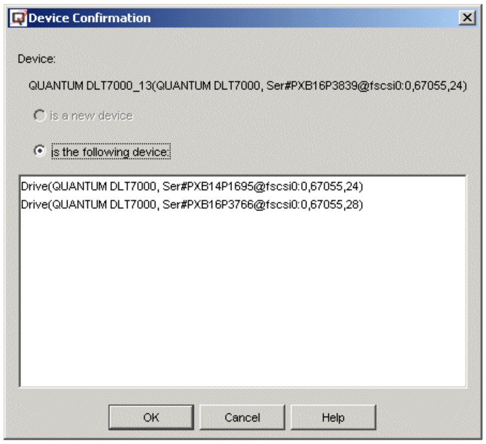
```
Libraries
  STK 9730_6(configured)
    LibraryController
      STK 9730_6(Scsi3:1,0,25)(amber.commvault.com)(configured, detect success)
      STK 9730_6(fscsi0:0,67055,25)(rolex.commvault.com)(configured, detect success)
    MasterPool_STK_9730_7(shared)(configured)
      DrivePool_STK_9730_16(rolex.commvault.com)(configured)
        (1) QUANTUM DLT7000_12(fscsi0:0,67055,28)(configured, detect success)
        (2) QUANTUM DLT7000_13(fscsi0:0,67055,24)(partially configu
      DrivePool_STK_9730_17(amber.commvault.com)(configured)
        (1) QUANTUM DLT7000_12(Scsi3:1,0,28)(configured, detect su
        (2) QUANTUM DLT7000_13(Scsi3:1,0,24)(partially configured, c
  StandAloneLibrary#(rolex.commvault.com)(not configured)
    MasterDrivePool#(shared)(not configured)
      DrivePool#(amber.commvault.com)(not configured)
        (1) QUANTUM DLT7000(Scsi3:1,0,24)(not configured, detect su
      DrivePool#(rolex.commvault.com)(not configured)
        (1) QUANTUM DLT7000(fscsi0:0,67055,24)(not configured, det
```

7. From the **Drive Properties** window, click the **Modify** button.

8. The following **Device Confirmation** window is displayed.

Note the following in the **Device Confirmation** window:

- The **Device** information contains the serial number of the old drive.
- The serial number for all the drives available in the library are displayed below the **is the following device** option.



Device:

QUANTUM DLT7000_13(QUANTUM DLT7000, Ser#PXB16P3839@fscsi0:0,67055,24)

○ is a new device

● is the following device:

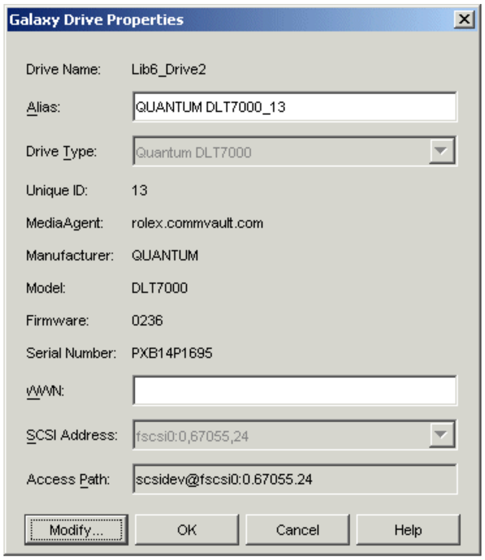
Drive(QUANTUM DLT7000, Ser#PXB14P1695@fscsi0:0,67055,24)
Drive(QUANTUM DLT7000, Ser#PXB16P3766@fscsi0:0,67055,28)

9. Click and highlight the new drive and then click **OK**.

Verify and ensure that you select the appropriate serial number associated with the newly replaced drive.

10. Click **OK** in the confirmation prompt.

The **Library Controller Properties** window gets updated with the **Serial Number** and **SCSI Address** of the new drive.



Drive Name: Lib6_Drive2

Alias: QUANTUM DLT7000_13

Drive Type: Quantum DLT7000

Unique ID: 13

MediaAgent: rolex.commvault.com

Manufacturer: QUANTUM

Model: DLT7000

Firmware: 0236

Serial Number: PXB14P1695

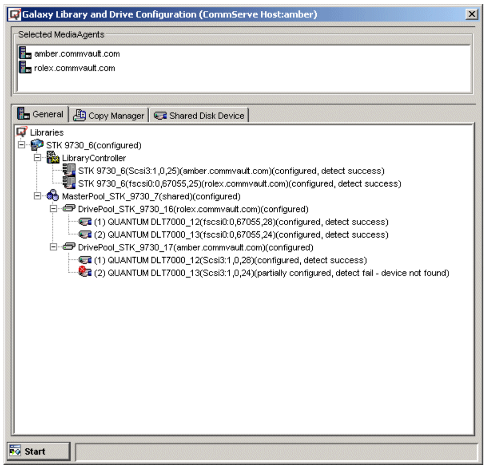
WWN:

SCSI Address: fscsi0:0,67055,24

Access Path: scsidev@fscsi0:0.67055.24

11. Click **OK**.

The new drive is replaced in the **Library and Drive Configuration** window.



amber.commvault.com
rolex.commvault.com

```
Libraries
  STK 9730_6(configured)
    LibraryController
      STK 9730_6(Scsi3:1,0,25)(amber.commvault.com)(configured, detect success)
      STK 9730_6(fscsi0:0,67055,25)(rolex.commvault.com)(configured, detect success)
    MasterPool_STK_9730_7(shared)(configured)
      DrivePool_STK_9730_16(rolex.commvault.com)(configured)
        (1) QUANTUM DLT7000_12(fscsi0:0,67055,28)(configured, detect success)
        (2) QUANTUM DLT7000_13(fscsi0:0,67055,24)(configured, detect success)
      DrivePool_STK_9730_17(amber.commvault.com)(configured)
        (1) QUANTUM DLT7000_12(Scsi3:1,0,28)(configured, detect success)
        (2) QUANTUM DLT7000_13(Scsi3:1,0,24)(partially configured, detect fail - device not found)
```

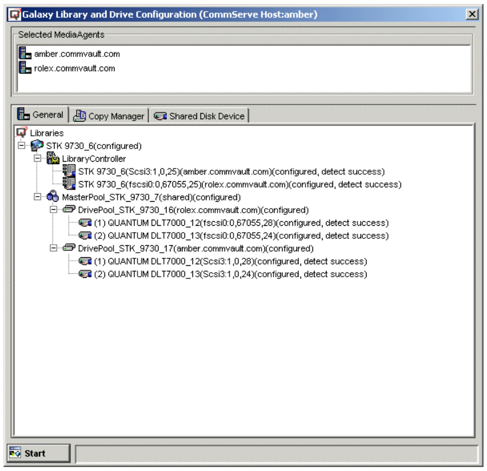
12. Repeat steps 6 to 11 to replace the drive in all the MediaAgents that are configured to access the library.

13. Perform an exhaustive detection of devices as described in Detect Devices Using Exhaustive Detection.

14. Configure the library as described in Configure Devices.

- In the **Configuration** window, select the **Library and all drives** option to configure the library.

This sample image displays the tree after the configuring the library.



```
amber.commvault.com
rolex.commvault.com
```

```
Libraries
  STK 9730_6(configured)
    LibraryController
      STK 9730_6(Scsi3:1,0,25)(amber.commvault.com)(configured, detect success)
      STK 9730_6(fscsi0:0,67055,25)(rolex.commvault.com)(configured, detect success)
    MasterPool_STK_9730_7(shared)(configured)
      DrivePool_STK_9730_16(rolex.commvault.com)(configured)
        (1) QUANTUM DLT7000_12(fscsi0:0,67055,28)(configured, detect success)
        (2) QUANTUM DLT7000_13(fscsi0:0,67055,24)(configured, detect success)
      DrivePool_STK_9730_17(amber.commvault.com)(configured)
        (1) QUANTUM DLT7000_12(Scsi3:1,0,28)(configured, detect success)
        (2) QUANTUM DLT7000_13(Scsi3:1,0,24)(configured, detect success)
```

REPLACE A DRIVE WITH A COMPATIBLE DRIVE TYPE IN THE SAN DDS ENVIRONMENT

The following procedure outlines the steps involved in replacing a drive with a compatible drive type to an existing library in the SAN environment, without deconfiguring the library.

Before you Begin

- The following process creates a new drive pool for the drive(s) that are replaced with a compatible drive type. As the number of configured drives in a drive pool cannot be smaller than the largest number of streams used by any storage policy that accesses that drive pool, verify and if necessary reduce the number of streams in storage policy copies to be equal to the number of functional drives in the drive pool.

  For example, assume that a drive pool containing four drives is accessed by a four-stream storage policy. If you wish to replace one of the drives with a compatible drive type, you must first reduce the four-streamed storage policies to three-streams.

  Previous database backups using multiple streams cannot be restored if the number of streams in a storage policy is reduced.

To replace a drive with a compatible drive type

1. Deconfigure the drive from all the MediaAgents that share the library.

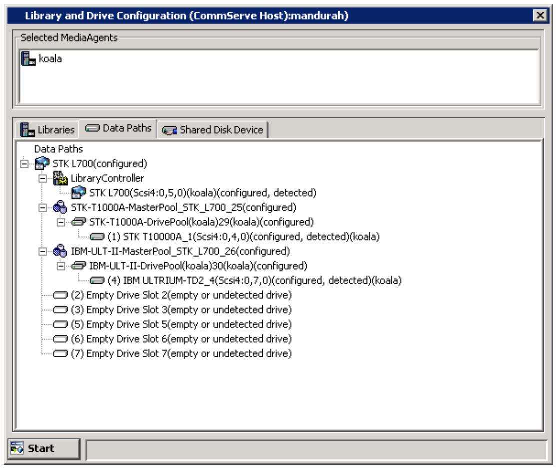
   From the **Library and Drive Configuration** window, right-click the drive you wish to deconfigure and then click **Deconfigure**.

   Click **Yes** in the confirmation prompt that appears.
2. Follow the procedure, Add a Compatible Drive Type in the SAN DDS Environment.

LIBRARY WITH MIXED DRIVE TYPES - POST CONFIGURATION CONSIDERATIONS

1. From the **CommCell Console**, create new scratch pool(s) in the library containing the mixed drive types.
   - If all of the drives use the same type of media, move some of the media into the new scratch pool.
   - If the drives use different media types, move all the media of a compatible type into the corresponding scratch pool.

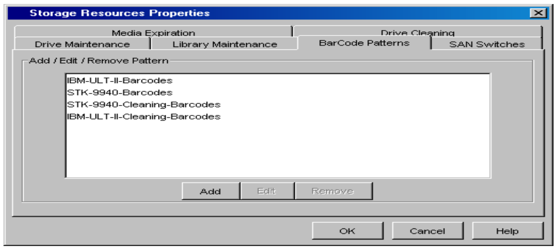
     You may have to physically inspect the media in the library to determine the media type.
2. Optionally, use appropriate names for the scratch pools, to avoid confusion.



Selected MediaAgents: koala

```
Data Paths
STK L700(configured)
    LibraryController
        STK L700(Scsi4:0,5,0)(koala)(configured, detected)
    STK-T1000A-MasterPool_STK_L700_25(configured)
        STK-T1000A-DrivePool(koala)29(koala)(configured)
            (1) STK T10000A_1(Scsi4:0,4,0)(configured, detected)(koala)
    IBM-ULT-II-MasterPool_STK_L700_26(configured)
        IBM-ULT-II-DrivePool(koala)30(koala)(configured)
            (4) IBM ULTRIUM-TD2_4(Scsi4:0,7,0)(configured, detected)(koala)
    (2) Empty Drive Slot 2(empty or undetected drive)
    (3) Empty Drive Slot 3(empty or undetected drive)
    (5) Empty Drive Slot 5(empty or undetected drive)
    (6) Empty Drive Slot 6(empty or undetected drive)
    (7) Empty Drive Slot 7(empty or undetected drive)
```

3. From the **CommCell Console**, create new Storage Policy Copies with proper naming conventions for easier identification, or re-associate existing Storage Policy Copies to use the appropriate scratch pools. This will ensure that the appropriate media is used in the respective drive.



Add / Edit / Remove Pattern

IBM-ULT-II-Barcodes
STK-9940-Barcodes
STK-9940-Cleaning-Barcodes
IBM-ULT-II-Cleaning-Barcodes

4. Whenever you import new media, physically inspect the media to determine the media type.

Perform one of the following steps, depending on whether the automatic media discovery option is enabled or disabled in the library:

- If the automatic media discovery option is enabled, move the respective media to the appropriate scratch pool from the **Default Scratch Pool**.
- If the automatic media discovery option is disabled, discover the respective media to the appropriate scratch pool.
- Verify and ensure that you select the appropriate scratch pool when you delete the contents of a media using the **Delete Contents** option.

Alternate Data Paths (GridStor) - Troubleshoot

Topics | How To | Troubleshoot | Examples | Support | Related Topics

No available data path candidates to add

This might occur for the following reason:

Cause: You may not have shared the index cache for the MediaAgent(s) that you wish to add as a data path candidate.

Solution: Check your criteria for using alternate data paths. (See Select the Criteria for using an Alternate Data Path for more information.)

Depending on the selected criteria, you may have to share the index cache for the MediaAgent(s). Share the index cache and then add the necessary data paths. See Index Cache for information on index cache sharing.

Backups fail with an Index Not Available error

This might occur for the following reason:

Cause: All the MediaAgents associated with the data path candidates may not be pointing to the same network share and the same folder within this network share for its index cache location..

Solution: For all the MediaAgents that are used as a data path candidate, open the Catalog tab of **MediaAgent Properties**, and verify whether the **Index Cache Directory** points to the same network share and the same folder within this network share for its index cache location.

Increased media usage, after establishing data paths in the CommCell

This might occur for the following reasons:

Cause: Fail over to data path candidates may be marking the media from last used library as *Appendable* resulting in partial usage of media.

Solution: Enable the option to reuse *Appendable* media, as described in Reuse Media Marked as Appendable.

Cause:

- If no alternate data paths are added in the primary copy, the number of streams may be more than the number of drives available in the library associated with the copy.
- If alternate data paths are added in the primary copy, the number of streams may be more than the sum of drives available in all the libraries associated with all the data paths in the copy.

Solution:

Reduce the number of streams to the following:

- If no alternate data paths are added, the number of streams must be equal to the number of drives in the library associated with the primary copy.
- If alternate data paths are added in the primary copy, the number of streams must be equal to the number of drives in all the libraries associated with all the data paths.

BACKUPS TO A STORAGE POLICY COPY WITH MULTIPLE DATA PATHS ARE IN THE WAITING STATE

This might occur for either of the following reason:

Cause: The criteria for using an alternate data path may not be selected.

Solution: Select the criteria for using an alternate data path as described in Select the Criteria for using an Alternate Data Path.

Cause: All the resources associated with all the data paths may not be available .

Solution: Verify the following resources and if possible enable the resources associated with at least one data path.

- MediaAgent Properties - verify the MediaAgents associated with the data paths are online.
- Library Properties - verify the libraries associated with the data paths are online.
- Drive Pool Properties - verify the drive pools associated with the libraries in the data path are online.
- Drive Properties - verify the drives associated with each of the drive pools in the data path are online.
- Also ensure that spare media is available in the scratch pools associated with the data paths added in the storage policy copy.

JOBS USING THE LIBRARY GO INTO WAITING

The **Reason for the Job Delay** in the **Job Details** dialog box may display the message *No Resource available*.

Cause: The **Device Streams** assigned in the Storage Policy Properties associated with the library is greater than the number of drives available in the library.

Solution: Make sure that the **Device Streams** assigned is equal to the number of drives in the library.

If you have added alternate data paths to the primary copy of the storage policy, the number of streams must be equal to the sum of drives available in all the libraries associated with all the data paths.

BACKUPS ON UNIX MEDIAAGENTS FAIL WITH AN INDEX NOT AVAILABLE ERROR

Cause: The mount point to the index cache folder may not be mounted. Note that mount points are not automatically mounted when a Unix MediaAgent is rebooted.

Solution:

1. From the Catalog tab of MediaAgent Properties, verify the location of the **Index Cache Directory** for the MediaAgent.
2. Mount the folder containing the index cache using the same path specified in **Index Cache Directory.**
3. Re-run the backup.

MULTI-STREAMED DATABASE BACKUPS ALWAYS REMAIN IN THE WAITING STATE

Cause:

You may have defined more number of streams than the actual number of drives in the library associated with the default data path candidate.

Solution:

1. Kill the backup job.
2. Reduce the number of streams in the Storage Policy Properties dialog box.
3. If necessary, reduce the number of streams in the Subclient Properties (Storage Device) tab, associated with the backup.
4. Re-run the backup.

Cause:

The resources on the default data path candidate may not be available and each of the alternate data paths do not have sufficient number of drives.

Solution:

1. Verify the following resources and enable the resources associated with the default data path.
   - MediaAgent Properties - verify the MediaAgents associated with the default data path is online.
   - Library Properties - verify the libraries associated with the default data path is online.
   - Drive Pool Properties - verify the drive pools associated with the libraries in the default data path is online..
   - Drive Properties - verify the drives associated with each of the drive pools in the default data path is online.
   - Also ensure that spare media is available in the scratch pools associated with the default data path.
2. Add an alternate data path with sufficient number of physical drives to support this backup.

BACKUPS DO NOT AUTOMATICALLY USE AN ALTERNATE DATA PATH SOON AFTER THE TIME INDICATED IN THE CRITERIA FOR ALTERNATE DATA PATH

This might occur for the following reasons:

Cause: The time indicated in the Criteria for Alternate Data Path, is the minimum time that the system will wait before using an alternate data path. The actual switch over will occur only when the backup job is processed by the Job Manager and depends on the number of jobs in the Job Manager at that time.

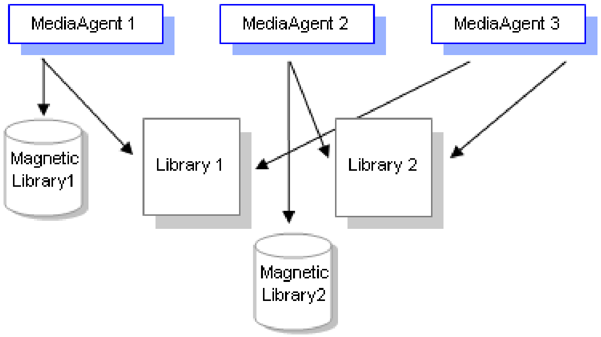
Solution: The backup job will automatically complete, when the Job Manager processes the job and the time indicated in the criteria for alternate data path is reached.

ALTHOUGH COMMON DATA PATHS ARE DEFINED IN PRIMARY AND SECONDARY COPIES, ANOTHER DATA PATH IS BEING USED FOR AUXILIARY COPY OPERATIONS

This might occur for the following reasons:

Cause: If alternate data paths are selected on secondary copies the system will always strive to perform LAN-free Auxiliary Copies.

Consider the diagram on the right. Using this configuration as an example, we can setup the following data paths:



Storage_policy_1= Primary Copy

MediaAgent 1, Library 1, Drive Pool 1, Default scratch Pool (Default path)

MediaAgent 2, Library 2, Drive Pool 2, Default scratch Pool (alternate path)

Storage_policy_1= Secondary Copy

MediaAgent 3, Library 1, Drive Pool 3, Default scratch Pool (Default path)

MediaAgent 3, Library 2, Drive Pool 4, Default scratch Pool (alternate path)

MediaAgent 1, Disk Library 1

MediaAgent 2, Disk Library 2

Assume that a full and incremental backup was performed. The data associated with the full backup resides in Library 1with media ID 0001. During the incremental backup the alternate data path was used and hence the incremental backup data resides in Library 2 with media ID 0002.

When an Auxiliary Copy operation is run on the secondary copy, MediaAgent 3 will be used to perform the operation. This is because MediaAgent 3 has access to both the libraries, and thus can read from media used by both MediaAgent 1 and MediaAgent 2.

Solution: This setup may be advantageous as it uses no network resources for the Auxiliary Copy operation. If however, you wish to remove this setup, remove the alternate data paths from the Secondary Copy.

ACCESS DENIED TO THE SHARED INDEX CACHE DIRECTORY

This might occur for either of the following reasons:

Cause: Trust relationships between the MediaAgent's domains and the domain in which the shared index cache resides may not be established.

Solution: Contact your Network Administrator to setup trust relationships between the domains.

UNABLE TO BROWSE DATA

Cause:

MediaAgent is not upgraded. An index cache entry created by a MediaAgent in the current version is accessed by a MediaAgent in the previous version.

Solution:

Upgrade the MediaAgent.

INDEX PROCESSING ON MEDIAAGENT FAILED DUE TO A CREATEINDEX PROCESSING ERROR

Cause:

MediaAgent is not upgraded. An index cache entry created by a MediaAgent in the current version is accessed by a MediaAgent in the previous version.

Solution:

Upgrade the MediaAgent.

Cleaning Media - Troubleshoot

Topics | How To | Troubleshoot | Related Topics

CLEANING MEDIA IS NOT RECOGNIZED

Cause: The cleaning media may have expired.

This may happen when the expired cleaning media is loaded in the drive by a data protection operation or a drive cleaning operation. In this situation you may see an error similar to the following:

```
The SCSI device reported that the source or target medium is not present. Please check to see if the Library Arm Changer and Drive is functioning correctly.
```

Solution: The unload operation may also fail. Hence physically remove the media from the drive. Use a new cleaning media to clean the drive. Make sure that the cleaning media is imported into the cleaning media pool.

Data Integrity Validation - Troubleshoot

Topics | How To | Troubleshoot | Related Topics

JOBS PENDING DUE TO DATA INTEGRITY VALIDATION ERROR

Cause:

Data Integrity Validation for the job has failed.

Action:

Review the error code and the description of the pending job to identify the reason for failure.

- If Data Integrity Validation on Network has failed, verify the network cord connecting the MediaAgent and the corresponding client. Replace the network cord, if necessary.
- If Data Integrity Validation on Media has failed, check the storage media device and replace the device if necessary.

See Handling Data Integrity Validation Errors for information on handling jobs pending due to Data Integrity Validation errors.

Drive Operations - Troubleshoot

Topics | How To | Troubleshoot | Related Topics

Drive requires cleaning

Solution:

- To automatically clean the drive, enable the **Enable Auto-Cleaning** option as described in Enable or Disable Automatic Drive Cleaning.
- If you wish to manually initiate the drive cleaning operation use one of the following methods:
  - Use the **Clean Drive** option as described in Clean Drive.
  - Use the library front panel options to clean the drive. In this case you must mark the drive as cleaned as described in Mark a Drive as Cleaned

DRIVE IS MARKED OFFLINE

This might occur for either of the following reasons: (Verify the drive **Offline Reason** as described in View the Drive Offline Reason.)

Cause: The drive maybe marked Offline by the user. The **Offline Reason** for the drive displays the following message:

```
No errors detected
```

Solution: Bring the drive online as described in Enable or Disable a Drive.

Cause: The drive may fail to initiate. The **Offline Reason** for the drive displays the following message:

```
Initialization in progress. Recovering drive state. Please wait
```

Solution: Wait a few minutes. The drive will be marked Online once the initialization process completes.

Cause: The drive may be marked as broken. The **Offline Reason** for the drive displays the following message:

```
Repeated errors during mounts and unmounts have now exceeded a threshold. The drive has been marked as broken. Please check your
hardware, firmware versions as well as cables/terminators/bent pins. Then mark the drive as fixed by right clicking on the drive
```

Solution: Detect and fix the hardware issues. Once the hardware is fixed, mark the drive as fixed as described in Mark a Drive as Fixed.

Cause: Media maybe stuck in the drive. The **Offline Reason** for the drive displays the following message:

```
There is a media stuck in the drive. An automatic recovery will be attempted. For manual recovery please try following steps. Reset
the drive from right click options and wait few minutes for it to become online. If it doesn't become online then attempt to reset the
entire library. If both fail, then inspect the drive for any hardware or firmware malfunction. Also verify your
cables/terminators/bent pins.
```

Solution: Follow the steps described in Media is stuck in a drive.

Cause: Drive may require cleaning. The **Offline Reason** for the drive displays the following message:

Drive indicates that cleaning is required. For a regular library ensure that you have cleaning tapes in the cleaning pool of the library. Then right click on the drive and choose clean option. For standalone, insert the cleaning tape into the drive manually and wait for it to unload after cleaning is completed. Then right click on the drive to mark it as cleaned.

Solution: Follow the steps described in Drive requires cleaning.

Cause: MediaAgent maybe Offline or unreachable. The **Offline Reason** for the drive displays the following message:

```
Cannot communicate with Bull Calypso Media Mount Manager Service. Please ensure that: The Media agent is reachable from CommServe. All
MediaAgent services are running.
```

Solution: Ensure that the MediaAgent is Online. Check and verify that the Bull Calypso `Media Mount Manager` is running. Check the communication between the MediaAgent and CommServe.

MEDIA IS STUCK IN A DRIVE

Solution:

To automatically recover stuck media, enable the **Enable stuck tape recovery** option as described in Enable or Disable Stuck Media Recovery.

If the stuck media fails to automatically recover, use the following options:

- Unload the drive as described in Unload a Drive.
- If the unload does not recover the stuck media, reset the drive as described in Reset a Drive.
- If the reset drive does not recover the stuck media, reset the library as described in Reset a Library.
- If all the above actions does not recover the stuck media, open the library door and manually remove the stuck media. Refer to the library manufacturer's documentation for information on recovering stuck media.

Index Cache - Troubleshoot

Topics | How To | Troubleshoot | Related Topics

LOGIN AND PASSWORD PROMPT IS ALWAYS DISPLAYED WHEN ACCESSING INDEX CACHE, DISASTER RECOVERY BACKUP AND/OR MOUNT PATH

This might occur for the following reason:

Cause:

You may be accessing an UNC path which is in different domain and that domain may not have trust relations established with the domain in which the computer is located. This results in the software prompting for User name and Password each time the UNC is accessed.

Solution:

Contact your Network Administrator to setup trust relationships between the domains.

ACCESS DENIED TO THE SHARED INDEX CACHE DIRECTORY

This might occur for either of the following reasons:

Cause: Trust relationships between the MediaAgent's domains and the domain in which the shared index cache resides may not be established.

Solution: Contact your Network Administrator to setup trust relationships between the domains.

UNABLE TO BROWSE DATA

Cause:

MediaAgent is not upgraded. An index cache entry created by a MediaAgent in the current version is accessed by a MediaAgent in the previous version.

Solution:

Upgrade the MediaAgent.

INDEX PROCESSING ON MEDIAAGENT FAILED DUE TO A CREATEINDEX PROCESSING ERROR

Cause:

MediaAgent is not upgraded. An index cache entry created by a MediaAgent in the current version is accessed by a MediaAgent in the previous version.

Solution:

Upgrade the MediaAgent.

Library and Drive Configuration - Troubleshoot

Topics | How To | Troubleshoot | Related Topics

Device Detection on AIX MediaAgent is Slow

Unable to detect devices in Solaris

Unable to Detect Non-IBM Libraries on AIX

Non-IBM Libraries are not Configurable in an LPAR Environment

Device Detection on AIX MediaAgent is Slow

This might occur for the following reason:

Cause: On AIX MediaAgents, the presence of a number of SCSI adaptors may result in slowing down the detection process. If you know that some of these adaptors are not required by the MediaAgent, you can skip them during the detection process as described in below.

Create the following file:

`<software installation path>/Base/detectdevices.skip`

Use the following format to add the list of adapters that must be skipped during device detection.

`adapter <adapter name>`

For example:

```
adapter scsi2

adapter fscsi1
```

Note the following:

- Entries are case-sensitive
- Adapters to be skipped can be specified in any order
- Each entry must identify a single adapter to be skipped

Unable to Detect the Devices in Solaris

- If you have the `QLOGIC Sun FC HBA` with Sun drivers (`qlgc driver by SUN`), you may not be able to detect the devices from the **Library and Drive Configuration** window. Use one of the following procedures to attach the WA Driver to the Solaris MediaAgent in the above environment:
  - To attach the wa drivers when the library is attached to QLOGIC FC HBA by SUN
  - To attach the `wa` drivers when the library is attached to QLOGIC FC HBA by SUN with a storage router
- Your devices may have LUNS greater than 7. Follow the procedure described in To Scan Devices with LUNs greater than 7 to correct this problem.

To Attach the wa Drivers When the Library is Attached to QLOGIC FC HBA by SUN

1. Ensure that the tape devices are visible to the Solaris kernel.

   You can do this using the following commands:

   ```
   Run cfgadm -al

   grep/look for type as tape devices
   ```

   If (`cfgadm -al`) displays all the devices configured on system, look for the word tape to identify `tape` devices.

   For example, the output of the `cfgadm -al` command may be as follows:

   ```
   Ap_Id                                Type           Receptacle     Occupant       Condition
   c0                                   scsi-bus       connected      configured     unknown
   c0::dsk/c0t0d0                       disk           connected      configured     unknown
   c0::dsk/c0t10d0                      disk           connected      configured     unknown
   c0::dsk/c0t6d0                       CD-ROM         connected      configured     unknown
   c0::dsk/c0t8d0                       disk           connected      configured     unknown
   ```

```
c0::dsk/c0t9d0                       disk          connected     configured     unknown
c3                                   scsi-bus      connected     unconfigured   unknown
c6                                   fc-fabric     connected     configured     unknown
c6::100000d08000167d                 tape          connected     configured     unknown
c6::100000d080001986                 tape          connected     configured     unknown
c6::100000e00221b69                  array-ctrl    connected     unconfigured   unknown
c6::100000e00221d909                 disk          connected     unconfigured   unknown
c6::2100002037194c51                 disk          connected     configured     unknown
c6::210000203719599e                 disk          connected     configured     unknown
c7                                   fc            connected     unconfigured   unknown
c8                                   fc            connected     unconfigured   unknown
```

If you do not see the devices as shown in the above example, make sure that the devices are visible to the Solaris kernel before proceeding any further.

2. If you see the tape devices, as shown in the above example, run the following script:

   ***<software installation path>*/WA/wa_sunqlc_add**

   After running the script, you will be able detect the devices from the `Library and Drive Configuration` window.

TO ATTACH THE WA DRIVERS WHEN THE LIBRARY IS ATTACHED TO QLOGIC FC HBA BY SUN WITH A STORAGE ROUTER

1. Ensure that the tape devices are visible to the Solaris kernel.

   You can do this using the following commands:

   ```
   Run cfgadm -al
   ```

   ```
   grep/look for type as array-ctrl
   ```

   For example, the output of the `cfgadm -al` command would be as follows:

   ```
   c6::100000e00221b691 array-ctrl  connected    unconfigured  unknown
   ```

   If you do not see the devices as shown in the above example, make sure that the devices are visible to the Solaris kernel before proceeding any further.

2. If you see the `array-ctrl` as shown in the above example, you will have to add the necessary information in the following file:

   ```
   /usr/kernel/drv/wa.conf
   ```

3. Add the necessary entries using the following pattern to add each device.

   ```
   name="wa" parent="fp" target=16 lun=0 fc-port-wwn="WWPN"
   ```

   Using the above example, it will be as follows:

   ```
   name="wa" parent="fp" target=16 lun=0 fc-portwwn="100000e00221b691"
   ```

   Add 8 entries from lun=0-7

   Example:

   ```
   name="wa"        parent="fp"      target=16        lun=0            fc-port-wwn="100000e00221b691";
   name="wa"        parent="fp"      target=16        lun=1            fc-port-wwn="100000e00221b691";
   name="wa"        parent="fp"      target=16        lun=2            fc-port-wwn="100000e00221b691";
   name="wa"        parent="fp"      target=16        lun=3            fc-port-wwn="100000e00221b691";
   name="wa"        parent="fp"      target=16        lun=4            fc-port-wwn="100000e00221b691";
   name="wa"        parent="fp"      target=16        lun=5            fc-port-wwn="100000e00221b691";
   name="wa"        parent="fp"      target=16        lun=6            fc-port-wwn="100000e00221b691";
   name="wa"        parent="fp"      target=16        lun=7            fc-port-wwn="100000e00221b691";
   ```

4. Save the changes.

5. Stop the services in the MediaAgent in which the entries were added.

6. Execute the following commands to create the device nodes:

   ```
   rem_drv wa
   ```

   ```
   add_drv wa
   ```

7. Start the services in the MediaAgent in which the entries were added.

   You will now be able detect the devices from the `Library and Drive Configuration` window.

TO SCAN DEVICES WITH LUNS GREATER THAN 7

By default the MediaAgent scans for devices with LUNs 0-7. If the devices are over these values they will not be detected. Perform the following steps to correct this problem:

1. Edit the following file:

   ```
   /usr/kernel/drv/wa.conf
   ```

2. Add an additional line across all targets to add a specific LUN. For example, to add LUN 8 and assuming that you have one target - Target 0 - you need the following line:

   ```
   name="wa" class="scsi" target=0 lun=8;
   ```

UNABLE TO DETECT NON-IBM LIBRARIES ON AIX

CAUSE

By default, AIX does not have a driver that attaches to non-IBM libraries. The driver provided by IBM, Atape, attaches only to IBM libraries.

SOLUTION

- If you have AIX 5.3 (maintenance level 5 and above), AIX 6.1 or AIX 7.1, use the following procedure to detect any non-IBM libraries that are not detected.
- If you have IBM only libraries connected to the MediaAgent, install the IBM Atape driver on this MediaAgent and proceed to step 11.

  Arm-changer will be detected as smcX device (where X=1,2,3...).

1. Ensure that no jobs are running in the CommCell Console.

2. Stop the Calypso services on this MediaAgent.

3. Run `cfgmgr` command to configure devices currently detected by the OS.

If the adapter ID is known, use the -l option to limit action to adapter.

```
cfgmgr -v
```

4. Navigate to **<Software_Installation_Path>/Base** folder.

Run the following command:

```
cd <Software_Installation_Disc>/Base
```

5. Determine device details for currently detected devices. This information will be used to discover the library inquiry string.

```
Run ./detectdevices -add tape
```

Messages similar to the following will be displayed

```
----------------------------------------
scsi3 rmt0.1 5 0 pthru_adapter tape
scsi3 gnode0 5 1 pthru_adapter tape
fscsi0 rmt1.1 131328 0 pthru_adapter tape
fscsi0 rmt2.1 131584 0 pthru_adapter tape
fscsi0 smc0 131584 1 pthru_adapter tape
fscsi0 rmt3.1 131840 0 pthru_adapter tape
```

Note down the above device details for drive:

```
adapter - fscsi0, device - rmt1.1, target -
131328, Lun - 0
```

6. Navigate to **<Software_Installation_Path>/MediaAgent** folder.

7. Run test inquiry (**testinq**) command.

- To determine the library's inquiry string, you may need to run the **testinq** command on the next or previous LUN of the drive device found.

  Run this command till the **Device Type** option in the result displays **8**. If the **Device Type** is displayed as **8** then it confirms that this device is an arm-changer.
- For example, if the drive above in **step 5** was found on adapter `fscsi0`, target `131328`, LUN `0`, then the **testinq** command may be issued on LUN `1`.

  When **Device Type 8** is discovered, the library's inquiry string is defined by characters 9-24 following the "**:**". Within this example, inquiry string is "**Scalar i500   **".

  - It may be necessary to run the **testinq** command on both, the next Target and LUN for SAS devices.
  - Note that the inquiry string is case and space sensitive.

```
Run ./testinq /dev/fscsi0 131328 1
/dev/fscsi0@131328,1:ADIC    Scalar i500
600G|Serial# ADICA0C0035914_LLB |Device Type 8
```

8. Run `ksh ./removegnode.ksh`

```
# ksh ./removegnode.ksh
```

```
Before proceeding, please make sure Calypso
services are shutdown

Hit enter to continue

0518-307 odmdelete: 0 objects deleted.

0518-307 odmdelete: 0 objects deleted.

0518-307 odmdelete: 0 objects deleted.

0518-307 odmdelete: 0 objects deleted.
```

9.

- If detecting a SAS non-IBM library for the first time, run the following command:

  Run `ksh ./addSASgnodestring.ksh`

  You need to provide library's inquiry string. From the previous **testinq** result in step 7, enter **Scalar i500**. The script will pad out this string so 16 characters total are entered.

  Continue to step 11.

- If adding a SCSI, FC or additional SAS non-IBM library:

  Edit the `gnode.Pdat.withatape` file to add new entry that will define the 16 characters of the library inquiry string.

  Make the entry for the appropriate adapter type (SCSI, FC, SAS).

  > Make sure that the inquiry string is prefixed with 1010, and is exactly 16 characters wide excluding the prefix. If the inquiry string is less than 16 characters, the remaining characters must be padded with spaces.

Example of `gnode.Pdat.withatape` file entries

This example illustrates entries, using Scalar i500 library for various adapter types.

ENTRY FOR SCSI LIBRARY

```
PdAt:
uniquetype = "tape/scsi/gnode"
attribute = "model_map"
deflt = "1010Scalar i500     " /* The model
number should be prefixed with 1010 and must be
exactly 16 characters long
excluding the prefix*/
values = ""
width = ""
type = "R"
generic = ""
rep = "s"
nls_index = 0
```

ENTRY FOR FC LIBRARY

```
PdAt:
uniquetype = "tape/fcp/gnode"
attribute = "model_map"
deflt = "1010Scalar i500     " /* The model
number should be prefixed with 1010 and must be
exactly 16 characters long
excluding the prefix */
values = ""
width = ""
type = "R"
generic = ""
rep = "s"
nls_index = 0
```

ENTRY FOR SAS LIBRARY

```
PdAt:
uniquetype = "tape/SAS/gnode"
attribute = "model_map"
deflt = "1010Scalar i500     " /* The model
number should be prefixed with 1010 and must be
exactly 16 characters long
excluding the prefix */
values = ""
width = ""
type = "R"
generic = ""
rep = "s"
nls_index = 0
```

10. Run `ksh ./addgnode.withatape.ksh`

```
ksh ./addgnode.withatape.ksh

Before proceeding, please make sure Galaxy
services are shutdown

Hit enter to continue
```

11. Rerun `cfgmgr` command to check if the library is detected.

Once `cfgmgr` has completed, check if the arm changer is detected using:

`lsdev -Cc tape` command

Arm-changers detected for non-IBM libraries are represented by `gnode` devices in the `lsdev -Cc tape` output.

```
cfgmgr -v

lsdev -Cc tape
```

Messages similar to the following will be displayed

Take note of the new gnodeX device listed below.

`gnode0 Available 10-70-00-5,1 Other SCSI Tape Drive`

gnode1 `Available 20-58-02 Other FC SCSI Tape`

```
Drive

rmt0 Available 10-70-00-5,0 Other SCSI Tape
Drive

rmt1 Available 20-58-02 LTO Ultrium Tape Drive
(FCP)

rmt2 Available 20-58-02 IBM 3580 Ultrium Tape
Drive (FCP)

rmt3 Available 20-58-02 Other FC SCSI Tape
Drive

smc0 Available 20-58-02 IBM 3576 Library Medium
Changer (FCP)
```

12. Restart the Calypso services on this MediaAgent.

EXAMPLE

This example illustrates the procedure for the Scalar i500 library (FC adapter)

```
# calypso stop

# cfgmgr -v

# cd <Software Installation Path>/Base

# ./detectdevices -add tape

  fscsi0 rmt1.1 131328 0 pthru_adapter tape

# cd <Software Installation Path>/MediaAgent

# ./testinq /dev/fscsi0 131328 1

  /dev/fscsi0@131328,1:ADIC    Scalar i500     600G|Serial# ADICA0C0035914_LLB |Device Type 8

  * Will need to add “Scalar i500     “ inquiry string to the gnode.Pdat.withatape file.
```

Insert entry into the file `gnode.Pdat.withatape` as given below:

ENTRY FOR SCSI LIBRARY

```
PdAt:

uniquetype = "tape/fcp/gnode"
attribute = "model_map"
deflt = "1010Scalar i500     " /* The model number should be prefixed with 1010 and must be exactly 16 characters long

excluding the prefix*/
values = ""
width = ""
type = "R"
generic = ""
rep = "s"
nls_index = 0
```

```
# ./removegnode.ksh

# ./addgnode.withatape.ksh

  Before proceeding, please make sure Galaxy services are shutdown

  Hit enter to continue

# cfgmgr -v

# lsdev -Cc tape

  gnode1 Available 20-58-02 Other FC SCSI Tape Drive

  rmt1 Available 20-58-02 LTO Ultrium Tape Drive (FCP)

# calypso start
```

NON-IBM LIBRARIES ARE NOT CONFIGURABLE IN AN LPAR ENVIRONMENT

To configure non-IBM libraries in an LPAR environment, install the latest service pack and then follow the steps described in Unable to Detect Non-IBM Libraries on AIX procedure to detect any non-IBM libraries that are not detected.

Library Operations - Troubleshoot

Topics | How To | Troubleshoot | Related Topics

None of my library controllers are active

Mount error while using brand new media or media from other applications

Jobs Using the library go into Waiting

Library is marked offline after turning off and turning on the library

Job failure due to mount media failure

Library reading all barcodes differently after firmware upgrades or when hardware was replaced

Adjust Timeout Value for SCSI Commands on UNIX MediaAgents

None of my library controllers are active

This might occur for either of the following reasons:

Cause: The Library Controller may not be enabled. When this happens the **Enabled** status is displayed as *NO* in the Library Controller Details dialog box.

Solution: Enable the library by clicking the **Enabled** option in the **Failover Library Controllers** pane in the Library Properties (Library Controller) dialog box.

Cause: The library may fail to initiate. This can happen when the library is performing a stuck tape recovery operation, scan or inventory operation, etc. When this happens the **Soft State** will be displayed as *OFF* in the Library Controller Details dialog box.

Solution:

- Wait until the library completes the operation. Refresh the CommCell Console (by pressing F5) and then verify whether the **Soft State** is indicated as *ON*.
- If the **Soft State** continues to be *OFF*, reset the library as described in Reset a Library. When the library comes online after completing the reset operation, refresh the CommCell Console (by pressing F5) and then verify whether the **Soft State** is indicated as *ON*.
- If the **Soft State** continues to be *OFF*, reset the library using the library's front-panel and once the reset operation completes, verify and ensure that the library is visible to the operating system. Refresh the CommCell Console (by pressing F5) and then verify whether the **Soft State** is indicated as *ON*.

Mount error while using brand new media or media from other applications

This might occur for the following reason:

Cause: You may be using brand new media (e.g., AIT-3) or media from another application using a different block size.

Solution: Overwrite the media as described in Reuse Media with Failed Content Verification.

Jobs Using the library go into Waiting

The **Reason for the Job Delay** in the **Job Details** dialog box may display the message *No Resource available*.

Cause: The **Device Streams** assigned in the Storage Policy Properties associated with the library is greater than the number of drives available in the library.

Solution: Make sure that the **Device Streams** assigned is equal to the number of drives in the library.

If you have added alternate data paths to the primary copy of the storage policy, the number of streams must be equal to the sum of drives available in all the libraries associated with all the data paths.

Library is marked offline after turning off and turning on the library

Cause: The library may not be visible to the operating system. This happens especially in Windows 2000, where the operating system automatically detects that the device is disconnected and therefore removes it from the device list.

Solution: Redetect the device from the Operating System. In some situations, you may have to reboot the computer to successfully redetect the device.

Job Failure Due to Mount Media Failure

Cause: Jobs fail when a mount media operation fails in the library.

Solution: You can configure the MediaAgent software to retry a specified number of times in the specified time interval, by creating the following registry keys:

- DataMoverMaxMountRetryValue
- DataMoverMaxMountRetrySleepTime

LIBRARY READING ALL BARCODES DIFFERENTLY AFTER FIRMWARE UPGRADES OR WHEN HARDWARE WAS REPLACED

Cause: When a libraries firmware is upgraded, or when a hardware is replaced a different barcode pattern may apply.

Solution:

- The system automatically updates the media barcodes if the **Automatically update barcodes on firmware changes option** is enabled in the **Advanced** tab of the **Library Properties**. (See Automatically update barcodes on firmware changes for more information.)
- If this option is disabled, and the barcodes are changed after a firmware upgrade all existing media, including media with data and spare media will be marked as exported and a new set of media (with new barcodes) will be listed inside the library. In this situation, you must update the barcodes as described in Manually Updating Media Barcodes after a Firmware Upgrade.

ADJUST TIMEOUT VALUE FOR SCSI COMMANDS ON UNIX MEDIAAGENTS

If you see devices timing out (in `MediaManager.log` file) and jobs failing as a result, you may want to adjust the timeout value for SCSI commands to these devices.

On Windows, the system uses native drivers and the timeout values are determined by the drivers.

On UNIX it's possible to specify timeout values for any SCSI command as long as the command is delivered using the pass-through driver as arm changers are always accessed using pass-through nodes on all UNIX platforms.

Tape drives by default are accessed using native drivers on AIX, Solaris, HP-UX, Linux and Tru64. Native drivers do not offer a way to customize SCSI timeouts. However, it is possible to enable pass-through mechanism from the CommCell Console by disabling the **Use Native device driver for data transfer for tape media** option in the **MediaAgent Properties**.

Once this is done pass through SCSI timeouts can be customized by modifying the following registry values:

```
/etc/CommVaultRegistry/Galaxy/Instance<xxx>/ScsiTimeouts

.internal.unique_id 1124467005_16773_40966_392845154

DEFAULT *120*

ERASE *18000*

INITIALIZE_ELEMENT_STATUS *600*

INITIALIZE_ELEMENT_STATUS_WITH_RANGE *600*

LOAD *900*

MOVE_MEDIUM *1500*

READ *900*

READ_ELEMENT_STATUS *600*

RESERVE *1200*

REWIND *1800*

SEEK_BLOCK *900*

SPACE *900*

WRITE *900*

WRITE_FILEMARKS *900*
```

These are the rules that should be observed while making the changes:

- All timeouts are in seconds.
- If a timeout is inside asterisks (e.g. *600*), it means that this is a default timeout. If you want to change the default value, you must remove the asterisks, or else the system will revert the timeout back to the default. This is done to simplify upgrades.
- If you want to change timeout for a command, which is explicitly listed in registry, you must put the new value on that respective line.

- If you want to change timeout for an unlisted command, you have two ways:
  - You can change the value for the DEFAULT timeout,
  - You can add the unlisted command by inserting a line like "CDB_XX <timeout>" where XX is the command's cdb[0] in hex.

MediaAgents - Troubleshoot

Topics | How To | Troubleshoot | Support | Related Topics

DEVICE DETECTION ON AIX MEDIAAGENT IS SLOW

This might occur for the following reason:

Cause: On AIX MediaAgents, the presence of a number of SCSI adaptors may result in slowing down the detection process. If you know that some of these adaptors are not required by the MediaAgent, you can skip them during the detection process as described in below.

Create the following file:

```
<software installation path>/Base/detectdevices.skip
```

Use the following format to add the list of adapters that must be skipped during device detection.

```
adapter <adapter name>
```

For example:

```
adapter scsi2

adapter fscsi1
```

Note the following:

- Entries are case-sensitive
- Adapters to be skipped can be specified in any order
- Each entry must identify a single adapter to be skipped

TAPE SPANNING FAILURE ON AIX MEDIAAGENTS WITH NATIVE DRIVERS

This might occur for the following reason:

Cause: On AIX MediaAgents with IBM library and ATAPE drivers and if **Use Native device driver for data transfer for tape media** option in the **MediaAgent Properties** is enabled, the MediaAgent software sets the drive attribute for `trailer_labels` to `yes` when a data protection operation is initiated. If this attribute is set to `no`, (For example, by other applications sharing the library) data protections operations may fail when the operation spans to another tape.

Use the following command to see the drive attribute for `trailer_labels`.

```
lsattr -El rmtX
```

JOB FAILURES IN SOLARIS MEDIAAGENTS USING NATIVE DRIVERS

Use the following steps if you find Data Protection Operation failing on Solaris MediaAgents when Native Drivers are enabled.

To configure native tape drive support on Solaris the native ST device nodes should be added to `/kernel/drv/st.conf` and bound to all the tape drive LUNs which are to be used.

For example:

Add the following lines in `/kernel/drv/st.conf` to bind tape drives having Target 0 and Lun 1, and Target 0 and Lun 2 with native driver:

```
name="st" class="scsi" target=0 lun=1;

name="st" class="scsi" target=0 lun=2;
```

Also make sure to reload the ST drivers using the following commands:

```
rem_drv st

add_drv st
```

ADJUST TIMEOUT VALUE FOR SCSI COMMANDS ON MEDIAAGENTS

If you see devices timing out (in `MediaManager.log` file) and jobs failing as a result, you may want to adjust the timeout value for SCSI commands to these devices.

- On Windows, the system uses native drivers and the timeout values are determined by the drivers.

  The SCSI timeout values may only apply to the SCSI commands associated to the library. The following are the SCSI timeout registry values that are available on Windows:

  ```
  HKEY_LOCAL_MACHINE\SOFTWARE\CommVault Systems\Galaxy\Instance<xxx>\ScsiTimeouts
  ```

  ```
  INITIALIZE_ELEMENT_STATUS    *600*
  INITIALIZE_ELEMENT_STATUS_WITH_RANGE *600*
  INQUIRY    *30*
  MOVE_MEDIUM    *1500*
  READ_ELEMENT_STATUS    *600*
  ```

- On UNIX it's possible to specify timeout values for any SCSI command as long as the command is delivered using the pass-through driver as arm changers are always accessed using pass-through nodes on all UNIX platforms.

  Tape drives by default are accessed using native drivers on AIX, Solaris, HP-UX, Linux and Tru64. Native drivers do not offer a way to customize SCSI timeouts. However, it is possible to enable pass-through mechanism from the CommCell Console by disabling the **Use Native device driver for data transfer for tape media** option in the **MediaAgent Properties**.

  Once this is done pass through SCSI timeouts can be customized by modifying the following registry values:

  ```
  /etc/CommVaultRegistry/Galaxy/Instance<xxx>/ScsiTimeouts
  ```

  ```
  .internal.unique_id 1124467005_16773_40966_392845154
  DEFAULT *120*
  ERASE *18000*
  INITIALIZE_ELEMENT_STATUS *600*
  INITIALIZE_ELEMENT_STATUS_WITH_RANGE *600*
  LOAD *900*
  MOVE_MEDIUM *1500*
  READ *900*
  READ_ELEMENT_STATUS *600*
  RESERVE *1200*
  REWIND *1800*
  SEEK_BLOCK *900*
  SPACE *900*
  WRITE *900*
  WRITE_FILEMARKS *900*
  ```

These are the rules that should be observed while making the changes:

- All timeouts are in seconds.
- If a timeout is inside asterisks (e.g. *600*), it means that this is a default timeout. If you want to change the default value, you must remove the asterisks, or else the system will revert the timeout back to the default. This is done to simplify upgrades.
- If you want to change timeout for a command, which is explicitly listed in registry, you must put the new value on that respective line.
- If you want to change timeout for an unlisted command, you have two ways:
  - You can change the value for the DEFAULT timeout,
  - You can add the unlisted command by inserting a line like "CDB_XX <timeout>" where XX is the command's cdb[0] in hex.

WORK-AROUND FOR A FAILED MEDIAAGENT

If a MediaAgent has failed and there are other MediaAgents in the CommCell, you can re-establish backup/restore operations for the affected client computers. Use any one of the following solutions.

To reestablish client operations when a MediaAgent has failed:

- Solution #1
- Solution #2
- Solution #3

SOLUTION#1

1. Create new storage policies where the primary copy transfers its backup data through a working MediaAgent and to a working library.
   - For tape libraries, ensure that the MediaAgent(s) that control both the library and target drive pool are in working order. (For shared libraries, different MediaAgents can control the library and a given drive pool. To identify these MediaAgents, check both the Library Properties and Drive Pool Properties dialog boxes.)
   - For disk libraries, ensure the MediaAgent that controls the disk library is in working order. (To identify the MediaAgent, check the related Library Properties dialog box.)
2. For each of the subclients of the affected client computers, perform the following:
   - From the CommCell Browser, open the Subclient Properties dialog box.
   - Click the Storage Devices tab and select one of the newly created storage policies.

Once the subclients of the affected client computers are associated to working libraries, you can resume backup operations.

SOLUTION#2

1. Use existing storage policies to back up the client computers that are affected by the failed MediaAgent. To do this, identify those storage policies where the primary copy transfers its backup data through a working MediaAgent and to a working library.
   - For tape libraries, ensure that the MediaAgent(s) that control both the library and target drive pool are in working order. (For shared libraries, different MediaAgents can control the library and a given drive pool. To identify these MediaAgents, check both the Library Properties and Drive Pool Properties dialog boxes.)
   - For disk libraries, ensure the MediaAgent that controls the disk library is in working order. (To identify the MediaAgent, check the related Library Properties dialog box.)
2. For each of the subclients of the affected client computers, perform the following:

   - From the CommCell Browser, open the Subclient Properties dialog box.
   - Click the Storage Devices tab and select one of the newly created storage policies.

Once the subclients of the affected client computers are associated to working libraries, you can resume backup operations.

SOLUTION#3

If a storage policy has a secondary copy and this copy points to another MediaAgent, and if Auxiliary Copies are performed regularly (therefore making available backed up data in an additional manner), promote the secondary copy to a primary copy.

MOVE A LIBRARY TO ANOTHER MEDIAAGENT WITHOUT DATA LOSS

In some situations you may have the need to move a library from one MediaAgent to another due to re-configuration or other requirements.

The following procedure provides step-by-step instructions on how to perform this operation.

1. Detach the library and attach it to the new MediaAgent and make sure that the hardware is visible to the operating system. See Driver Configurations for more information.
2. Open the CommCell Console and change the name of the MediaAgent associated with the library. See Change the MediaAgent (Host) Associated with a Library for more information.
3. If necessary run a quick backup to verify that the devices are functioning correctly.

Move a MediaAgent Without Data Loss

In some situations you may have the need to move a MediaAgent from one computer to another. For example:

- You may want to move the MediaAgent to another computer when you move the pilot version of the software to the production environment.
- You may want to separate the MediaAgent from a CommServe, if they were installed together.
- You may want to move a MediaAgent to a more powerful computer or such similar re-configuration needs.

You will require an additional MediaAgent license to perform this operation.

The following procedure provides step-by-step instructions on how to perform this operation.

1. Detach the library and attach it to the new computer and make sure that the hardware is visible to the operating system. See Driver Configurations for more information.
2. Install the MediaAgent software in the new computer. See MediaAgent Deployment for more information.
3. Open the CommCell Console and change the name of the MediaAgent associated with the library that was configured in the old MediaAgent. See Changing the MediaAgent (Host) Associated with a Library for more information.
4. If the index cache is configured in the old MediaAgent, move the index cache to the new MediaAgent. (See Move an Index Cache for step-by-step instructions.)
5. If necessary run a quick backup to verify that the devices are functioning correctly.
6. Uninstall the MediaAgent software from the original computer. See Uninstall Components for more information.

WARNING

Do not deconfigure the library at any point.

Also do not uninstall the old MediaAgent until the devices start functioning in the new MediaAgent.

Separate the CommServe from a CommServe-MediaAgent Computer

In some situations you may want to separate the CommServe from a MediaAgent computer, (with or without a File system *i*DataAgent) if they were installed together. For example, you may want to move the CommServe to a more powerful computer or such similar re-configuration needs.

The following procedure provides step-by-step instructions on how to perform this operation.

You can also use this procedure to relocate a CommServe and MediaAgent which are installed together, to two separate computers.

You will require an additional MediaAgent license to perform this operation.

SOURCE COMPUTER

1.	Copy the index cache folder (and the job results folder if the (File system *i*DataAgent is installed) to another location.	
2.	Perform a Disaster Recover Backup. Verify and ensure that the Disaster Recovery Backup completes successfully. Also note down the location of the disaster recovery backup file. (For a more detailed discussion, see Phases of Disaster Recovery Backups.)	See Starting a Disaster Recovery Backup for step-by-step instructions.
3.	Uninstall the software from the original computer.	See Uninstalling Components for more information.

WARNING

Do not deconfigure the libraries (tape/optical/disk libraries, etc.) when you uninstall the MediaAgent software.

ESTABLISHING THE NEW COMMSERVE COMPUTER

4.	Install only the CommServe software in the new computer.	See CommServe Deployment for information on installing the CommServe software.
5.	Restore the CommServe database using the CommServe Disaster Recovery Tool.	See Restore a Disaster Recovery Backup for step-by-step instructions.
6.	Change the name of the CommServe computer using the CommServe Disaster Recovery Tool.	See Change the Name of the CommServe Computer for step-by-step instructions.

7.	Inform the Client and MediaAgent computers of the new CommServe name. This can be done from the `CommCell Console`.	See Informing Clients of CommServe Name Change for step-by-step instructions.

ESTABLISHING THE NEW MEDIAAGENT COMPUTER

8.	Install only the MediaAgent software in the old computer. (You can also relocate the MediaAgent to another computer, if necessary.)	See MediaAgent Deployment for more information.
9.	During MediaAgent installation make sure to specify the index cache to the location in which it was copied in step 1. If you are unable to do so, perform the steps described in Manually Relocate the Index Cache.	
10.	Open the CommCell Console and change the MediaAgent name associated with the library.	See Changing the MediaAgent (Host) Associated with a Library for step-by-step instructions.
	If you have a disk library, make sure that the mount path is pointing to the appropriate location. If necessary move the mount path to the appropriate location and then change the location of the mount path.	See Move a Mount Path for step-by-step instructions.
11.	Deconfigure the original MediaAgent from the CommCell Console.	See Deconfigure a Client, MediaAgent, Agent, or Enabler for step-by-step instructions.

ESTABLISHING THE FILE SYSTEM *I*DATAAGENT IN THE MEDIAAGENT COMPUTER (IF IT WAS ORIGINALLY INSTALLED)

12.	Export the metadata records associated only with this client on the CommServe.	See Export Data from the Source CommCell for step-by-step instructions.
13.	Deconfigure the Client from the CommCell Console.	See Deconfigure a Client, MediaAgent, Agent, or Enabler for step-by-step instructions.
14.	Delete the Client in the CommCell Console.	See Delete a Client Computer for step-by-step instructions.
15.	Import the metadata records (that was exported in step 12) associated with the client computer in the CommServe.	See Import Data on the Destination CommCell for step-by-step instructions.
16.	Reinstall the file system *i*DataAgent on the computer.	See Deployment - Windows File System iDataAgent for more information.

Media Operations - Troubleshoot

Topics | How To | Troubleshoot | Related Topics

Media is marked as Expired

When a media exceeds the Media Expiration Thresholds the condition of the media is marked as *Expired* and the media is moved to **Expired Media** pool.

- You can view the Media Expiration Threshold Parameters from the Hardware Maintenance Thresholds (Media Expiration) dialog box.
- Verify the condition of the media as described in View the Condition of a Media.

Cannot find a media

Cause: The media may be exported or may have been moved to the Retired Media pool. In some situations, it may also be difficult to scan the media list, especially in libraries that have the capacity to store a large number of media.

Solution: Use the find media feature as described in Find a Media to search for a specific media.

Media Marked as Appendable is not Re-used

Solution: Check the **Use Appendable Media within n Day (s) of its last write time** option in the Library Properties (Media) tab to see if it is enabled. Also verify the number of days established for the option.

In addition note that the Appendable media is NOT selected for reuse only under the following conditions:

- When the media belongs to a different storage policy.
- If it was the last written media in that storage policy - in such a case, one spare media must be available before the system goes back to the appendable media. This is to ensure that the condition that caused the media to be skipped is cleared.
- Synthetic full backups will not use Appendable media.
- A job option which has the **Start New Media** option enabled, will not use appendable media.

Cleaning Media is Not Recognized

Cause: The cleaning media may have expired.

This may happen when the expired cleaning media is loaded in the drive by a data protection operation or a drive cleaning operation. In this situation you may see an error similar to the following:

```
The SCSI device reported that the source or target medium is not present. Please check to see if the Library Arm Changer and Drive is functioning correctly.
```

Solution: The unload operation may also fail. Hence physically remove the media from the drive. Use a new cleaning media to clean the drive. Make sure that the cleaning media is imported into the cleaning media pool.

Disk Libraries - Troubleshoot

Topics | Configure | How To | Troubleshoot | Related Topics

Mount failures in a job accessing a shared disk library

Verify whether the status of the disk library, mount path and the device are *Online*.

If the status is *Online*, this might occur for either of the following reason:

Cause: No drive letters are available in the operating system to mount the volume for the job.

Solution:

1. Ensure that there are sufficient drive letters available in the operating system for each device to mount the volume.
2. If all the drive letters are used, disconnect and make some drive letter available before resuming the job.

Login and Password prompt is Always displayed when Accessing Index Cache, Disaster Recovery Backup and/or Mount Path

This might occur for the following reason:

Cause:

You may be accessing an UNC path which is in different domain and that domain may not have trust relations established with the domain in which the computer is located. This results in the software prompting for User name and Password each time the UNC is accessed.

Solution:

Contact your Network Administrator to setup trust relationships between the domains.

Free Space Value for Mounted LUN Disk in Windows 2003 MediaAgent lists incorrectly

Cause:

When you use LUN Disk Array as UNC path from Windows 2003 machine, the free space from Windows 2003 machine is shown about parent directory instead of actual mounted LUN.

Solution:

User should share the mounted LUN and use that as the UNC path.

For example, if your disk array is mounted in remote machine **machine1** in **C:\** drive under **Folder1** as **C:\Folder1\LUN**. For Windows 2003 machine, when user uses UNC path **\\machine1\c$\Folder1\LUN** as mount path, the windows will display the free space available for **C** drive. Instead showing the free space of mount path. You have to share the folder **LUN** and use that as the UNC path e.g., **\\machine1\LUN**.

Mount paths configured on Isilon shares are marked offline

Cause

If you use an Isilon device to host a disk library, the mount path might go offline when the user name or password is changed.

Solution

Upgrade to the EMC Isilon OneFS operating system version 7.0.1.8 or later.

PnP (Plug and Play) Disk Libraries - Troubleshoot

Topics | Configure | How To | Troubleshoot | Related Topics

UNABLE TO VIEW THE PNP DISK IN COMMCELL CONSOLE

Check the following if you have plugged-in the PnP disk and do not automatically see the device displayed in the CommCell console:

- Check the **Check for media change in drive every n minutes** option in **Library Properties - Drive** tab to see how often the MediaAgent checks the drive for media changes in the drive.
  - See Setup Automatic Checking of Media for step-by-step instructions on how to modify this option.
  - See also Detecting Media Changes in Stand-Alone Drives for additional details.
- If the disk contains data and you wish to use the disk, verify and ensure that the **Only use PnP disk when it is blank** option is not enabled in the **Library Properties - Media Usage** tab. See Enable (or Disable) Option to Only Use Blank PnP Disks for step-by-step instructions.
- Verify the total capacity of the media and ensure that the disk size is greater than the value established in **Use disk only when the size is greater than (n) MB** option. If necessary modify the value to a smaller capacity so that the PnP disk is detected in the drive. See Enable (or Disable) the Option to Use PnP Disks with a Specific Size for step-by-step instructions.

PNP DISK IS DISPLAYED AS UNIDENTIFIED MEDIA IN THE COMMCELL CONSOLE

Blank disks are displayed as unidentified Media until a On Media Label (OML) is written on the media. If auto-stamping options are enabled the system writes an OML as soon as the media is detected. If auto-stamping options are not enabled the system writes an OML when a data protection job is initiated. You can also manually stamp the media and create an OML so that media is identified.

See Media Labeling in Stand-Alone Drives for more information.

SAN-Attached Libraries - Troubleshoot

Topics | Best Practices | Configure | How To | Troubleshoot | Related Topics

Unable to detect devices in Solaris

- To attach the wa drivers when the library is attached to QLOGIC FC HBA by SUN
- To attach the `wa` drivers when the library is attached to QLOGIC FC HBA by SUN with a storage router
- To Scan Devices with LUNs greater than 7

Job Failures in Solaris MediaAgents using Native Drivers

Backup Jobs from Windows 2003 Computers Fail in the SAN Environment

ScsiCmd Tool

Drive validation with Native Drivers on Solaris

UNABLE TO DETECT THE DEVICES IN SOLARIS

- If you have the `QLOGIC Sun FC HBA` with Sun drivers (`qlgc driver by SUN`), you may not be able to detect the devices from the **Library and Drive Configuration** window. Use one of the following procedures to attach the WA Driver to the Solaris MediaAgent in the above environment:
  - To attach the wa drivers when the library is attached to QLOGIC FC HBA by SUN
  - To attach the `wa` drivers when the library is attached to QLOGIC FC HBA by SUN with a storage router
- Your devices may have LUNS greater than 7. Follow the procedure described in To Scan Devices with LUNs greater than 7 to correct this problem.

TO ATTACH THE `WA` DRIVERS WHEN THE LIBRARY IS ATTACHED TO QLOGIC FC HBA BY SUN

1. Ensure that the tape devices are visible to the Solaris kernel.

   You can do this using the following commands:

   ```
   Run cfgadm -al
   ```

   ```
   grep/look for type as tape devices
   ```

   If (`cfgadm -al`) displays all the devices configured on system, look for the word tape to identify `tape` devices.

   For example, the output of the `cfgadm -al` command may be as follows:

   ```
   Ap_Id                         Type          Receptacle    Occupant      Condition
   c0                            scsi-bus      connected     configured    unknown
   c0::dsk/c0t0d0                disk          connected     configured    unknown
   c0::dsk/c0t10d0               disk          connected     configured    unknown
   c0::dsk/c0t6d0                CD-ROM        connected     configured    unknown
   c0::dsk/c0t8d0                disk          connected     configured    unknown
   c0::dsk/c0t9d0                disk          connected     configured    unknown
   c3                            scsi-bus      connected     unconfigured  unknown
   c6                            fc-fabric     connected     configured    unknown
   c6::100000d08000167d          tape          connected     configured    unknown
   c6::100000d080001986          tape          connected     configured    unknown
   c6::100000e00221b69           array-ctrl    connected     unconfigured  unknown
   c6::100000e00221d909          disk          connected     unconfigured  unknown
   c6::2100002037194c51          disk          connected     configured    unknown
   c6::210000203719599e          disk          connected     configured    unknown
   c7                            fc            connected     unconfigured  unknown
   c8                            fc            connected     unconfigured  unknown
   ```

   If you do not see the devices as shown in the above example, make sure that the devices are visible to the Solaris kernel before proceeding any further.

2. If you see the tape devices, as shown in the above example, run the following script:

   <*software installation path*>/WA/wa_sunqlc_add

   After running the script, you will be able detect the devices from the `Library and Drive Configuration` window.

TO ATTACH THE WA DRIVERS WHEN THE LIBRARY IS ATTACHED TO QLOGIC FC HBA BY SUN WITH A STORAGE ROUTER

1. Ensure that the tape devices are visible to the Solaris kernel.

   You can do this using the following commands:

   ```
   Run cfgadm -al
   ```

   ```
   grep/look for type as array-ctrl
   ```

   For example, the output of the `cfgadm -al` command would be as follows:

   ```
   c6::100000e00221b691 array-ctrl  connected    unconfigured  unknown
   ```

   If you do not see the devices as shown in the above example, make sure that the devices are visible to the Solaris kernel before proceeding any further.

2. If you see the `array-ctrl` as shown in the above example, you will have to add the necessary information in the following file:

   ```
   /usr/kernel/drv/wa.conf
   ```

3. Add the necessary entries using the following pattern to add each device.

   ```
   name="wa" parent="fp" target=16 lun=0 fc-port-wwn="WWPN"
   ```

   Using the above example, it will be as follows:

   ```
   name="wa" parent="fp" target=16 lun=0 fc-portwwn="100000e00221b691"
   ```

   Add 8 entries from lun=0-7

   Example:

   ```
   name="wa"          parent="fp"        target=16          lun=0              fc-port-wwn="100000e00221b691";
   name="wa"          parent="fp"        target=16          lun=1              fc-port-wwn="100000e00221b691";
   name="wa"          parent="fp"        target=16          lun=2              fc-port-wwn="100000e00221b691";
   name="wa"          parent="fp"        target=16          lun=3              fc-port-wwn="100000e00221b691";
   name="wa"          parent="fp"        target=16          lun=4              fc-port-wwn="100000e00221b691";
   name="wa"          parent="fp"        target=16          lun=5              fc-port-wwn="100000e00221b691";
   name="wa"          parent="fp"        target=16          lun=6              fc-port-wwn="100000e00221b691";
   name="wa"          parent="fp"        target=16          lun=7              fc-port-wwn="100000e00221b691";
   ```

4. Save the changes.

5. Stop the services in the MediaAgent in which the entries were added.

6. Execute the following commands to create the device nodes:

   ```
   rem_drv wa
   ```

   ```
   add_drv wa
   ```

7. Start the services in the MediaAgent in which the entries were added.

   You will now be able detect the devices from the `Library and Drive Configuration` window.

TO SCAN DEVICES WITH LUNS GREATER THAN 7

By default the MediaAgent scans for devices with LUNs 0-7. If the devices are over these values they will not be detected. Perform the following steps to correct this problem:

1. Edit the following file:

   ```
   /usr/kernel/drv/wa.conf
   ```

2. Add an additional line across all targets to add a specific LUN. For example, to add LUN 8 and assuming that you have one target - Target 0 - you need the following line:

   ```
   name="wa" class="scsi" target=0 lun=8;
   ```

JOB FAILURES IN SOLARIS MEDIAAGENTS USING NATIVE DRIVERS

Use the following steps if you find Data Protection Operation failing on Solaris MediaAgents when Native Drivers are enabled.

To configure native tape drive support on Solaris the native ST device nodes should be added to `/kernel/drv/st.conf` and bound to all the tape drive LUNs which are to be used.

For example:

Add the following lines in `/kernel/drv/st.conf` to bind tape drives having Target 0 and Lun 1, and Target 0 and Lun 2 with native driver:

```
name="st" class="scsi" target=0 lun=1;

name="st" class="scsi" target=0 lun=2;
```

Also make sure to reload the ST drivers using the following commands:

```
rem_drv st

add_drv st
```

Backup Jobs from Windows 2003 Computers Fail in the SAN Environment

SOLUTION:

Create the `AutoRunAlwaysDisable` registry key on all Windows 2003 computers that have access to the library in the SAN environment. For a detailed description of this problem and the registry key refer to the following article published in the Microsoft web site:

```
http://support.microsoft.com/default.aspx?scid=kb;en-us;842411&Product=w
```

ScsiCmd Tool

The ScsiCmd Tool is used to test whether the hardware supports SCSI-3 reservation. (SCSI-3 reservation is used when you enable the `Use SCSI Reserve for contention resolution` option in the **Library Properties** dialog box.) This tool is installed along with the MediaAgent software and available on all the MediaAgent computers.

For comprehensive information on using ScsiCmd Tool, see ScsiCmd Tool.

Drive Validation With Native Drivers on Solaris

By default, tape driver on Solaris, **st**, uses SCSI-2 reserve/release. When enabled, this conflicts with the SCSI-3 reserve/release done by the MediaAgent and the data protection operations wait indefinitely with the following message in the log file. (`dmWriter.log` or `cvd.log`)

```
1832 17 06/13 12:51:08 64  [] [DM_BASE    ] 43-41 Trying to create archive file : afileId = 52, ArchiveFileSeqNo = 0,FirstChunkSeqNo= 0
1832 17 06/13 12:51:09 64  [] [DM_BASE    ] 43-41 The size of the chunk will be around 4096 MB
1832 17 06/13 12:51:09 64  [] [DM_BASE    ] 43-41 Creating new chunk chunk id 102 VolId= 6 after setting the volume id for the chunk in
1832 17 06/13 12:51:10 64  [] [MEDIAFS    ] 43-41 Starting FM = 9. Hardware compression [1]
1832 17 06/13 12:51:10 64  [] [MEDIAFS    ] 43-41 Write Cached_filemark =9. Read Cached Filemarker [-1] Current_filemark = 9
1832 17 06/13 12:51:10 64  [] [MEDIAFS    ] 43-41 Trying to rewind two  filemarks behind the current position
```

To prevent this, SCSI-2 reserve/release must be turned off in the st driver. This can be done by adding a configuration entry `tape-config-list` in the `st.conf` (located under /kernel/drv directory).

For example:

If you have IBM ULTRIUM-TD3 drives connected to the Solaris system, the following line can be added to the `tape-config-list` entry in the `st.conf file` to prevent reserve/release from the st driver for the above drive type. If there is no `tape-config-list`, add it to the `st.conf`.

```
tape-config-list = "IBM ULTRIUM-TD3", "IBM ULTRIUM-TD3", "IBM-ULTRIUM-TD3";

IBM-ULTRIUM-TD3 = 2,0x3b,0,0x3865B,4,0x00,0x00,0x00,0x00,0,120,120,3600,3600,360 0,3600,3600;
```

For detailed information on the format of `st.conf` file, refer to **man st(7D)** or the `st.conf` file itself.

Stand-Alone Drives - Troubleshoot

Topics | Configure | How to | Troubleshoot | Related Topics

CLEANING STAND-ALONE DRIVES

Cause: A stand-alone drive indicates that the drive requires cleaning.

Solution: You must manually clean the stand-alone drives, whenever necessary. The `Clean Drive` option is not available for stand-alone drives (see Drive Cleaning for more information). However, after manually cleaning the stand-alone drives, you must mark the drive as cleaned as described in Mark a Drive as Cleaned . This will reset the counters that keep track of the number of drive events that have occurred since the drive was cleaned.

REUSE MEDIA WITH FAILED CONTENT VERIFICATION

Required Capability: See Capabilities and Permitted Actions

Use the following procedure to overwrite media in situations where the MediaAgent fails to read a media, e.g., incompatible data formats, etc.

To reuse media with failed content verification:

1. From the CommCell Browser, right-click the library for which you wish to reuse media with failed content verification, and then click **Properties**.
2. Click the Media tab.
3. From the **Overwrite Media** region, click **When Content Verification Failed.**
4. Click **OK** to save the changes.

ScsiCmd Tool

OVERVIEW

The ScsiCmd Tool is used to test whether the hardware supports SCSI-3 reservation. (SCSI-3 reservation is used when you enable the `Use SCSI Reserve for contention resolution` option in the **Library Properties** dialog box.) This tool is installed along with the MediaAgent software and available on all the MediaAgent computers.

The following section provides the steps for using this tool.

USING SCSICMD TOOL

1. Navigate to the <*software installation path*>\Base folder and double-click **ScsiCmdTool.exe**.

Press **<Enter>** twice to display the main menu and then choose **1** to read the devices.

```
There are currently 0 SCSI or Fibre-Channel Devices in our
list.
You can update the list by selecting items 1-3 below.
Or hit 4 to proceed to device operation menu.
  1.  Perform a quick bus scan
  2.  Perform an extensive bus scan
  3.  Select a device for testing.

  0.  Exit
Operation [1]:
```

2. Press **<Enter>** to continue.

The tool detects the devices and a message similar to the one shown in the sample, will be displayed.

Press **<Enter>** to continue.

```
We're ready to scan for all connected SCSI and Fibre
Channel devices now.
Note that on some systems (notably AIX) it may take
minutes to complete
so please be patient!

Press <ENTER> to begin the scan ...

Scanning now ... done.

Successfully read 10 devices...

Press <ENTER> to continue ...
```

3. From the main menu, choose **3** to select a device for testing.

```
There are currently 10 SCSI or Fibre-Channel Devices in
our list.
You can update the list by selecting items 1-3 below.
Or hit 4 to proceed to device operation menu.
  1.  Perform a quick bus scan
  2.  Perform an extensive bus scan
  3.  Select a device for testing.

  0.  Exit
Operation [1]:3
```

4. From the next menu, choose **13** to query the data from the target.

```
Please pick an action for tape device scsidev@Scsi4:0.0.2
below:

   1. Send TEST_UNIT_READY command
   2. Send INQUIRY command
   3. Get SERIAL Number
   4. Send MODE_SENSE command
   5. Send LOAD/UNLOAD command
   6. Send REWIND command
   7. Reposition tape (SPACE command)
   8. WRITE data
   9. WRITE filemark
  10. READ data
  11. READ and display data block-by-block
  12. Get drive READ/WRITE Statistics.
  13. Persistent Reserve In.
  14. Persistent Reserve Out.
  15. Send arbitrary SCSI command.

  0. Select another SCSI device.

Operation [1]: 13
```

5. A list of devices will be displayed. Choose a device and then press **<Enter>** to continue.

The tool should display a message similar to the one shown in the sample. (Note that in some cases, a registered key may also be found.)

If the tool displays a message similar to the following, SCSI-3 is not supported by the device.

```
UXScsi::send(): INQUIRY SCSI command to scsidev@Scsi4:0.0.2 failed with
```

```
Get READ KEY or READ RESERVATION? [k]:
Counter: 1
No registered key has been found

Press <ENTER> to continue ...
```

```
error=Incorrect function
```

6. From the next menu, choose **14** to perform a task in the target device.

```
Please pick an action for tape device scsidev@Scsi4:0.0.2
below:

   1. Send TEST_UNIT_READY command
   2. Send INQUIRY command
   3. Get SERIAL Number
   4. Send MODE_SENSE command
   5. Send LOAD/UNLOAD command
   6. Send REWIND command
   7. Reposition tape (SPACE command)
   8. WRITE data
   9. WRITE filemark
  10. READ data
  11. READ and display data block-by-block
  12. Get drive READ/WRITE Statistics.
  13. Persistent Reserve In.
  14. Persistent Reserve Out.
  15. Send arbitrary SCSI command.

  0. Select another SCSI device.

Operation [1]: 14
```

7. From the next menu, choose **7** and make sure that it executes successfully, as shown in the sample image.

```
1.Register    2.Reserve    3.Release
4.Clear       5,Prempt     6.Prempt And Abort
7.Register And Ignore Key

Please enter a service action? [1]: 7

1.Write Exclusive(0x01)    2.Exculsive(0x03)
3.Write Exclusive RO(0x05) 4.Exclusive RO(0x06)
5.Write Exclusive AR(0x07) 6.Exclusive AR(0x08)

Please enter a access type? [1]: 2

Please enter a registered key?:

Please enter a service action key?: key1

Executing the command...

Successful
```

8. Again from the menu, choose **2** and make sure that it executes successfully.

```
1.Register    2.Reserve    3.Release
4.Clear       5,Prempt     6.Prempt And Abort
7.Register And Ignore Key

Please enter a service action? [1]: 2

1.Write Exclusive(0x01)    2.Exculsive(0x03)
3.Write Exclusive RO(0x05) 4.Exclusive RO(0x06)
5.Write Exclusive AR(0x07) 6.Exclusive AR(0x08)

Please enter a access type? [1]: 3

Please enter a registered key?: key2

Please enter a service action key?:

Executing the command...

Successful
```

9. Execute the `Persistent Reserve In` described in step 4 and 5 and make sure that the key is reserved.

```
Get READ KEY or READ RESERVATION? [k]:
Counter: 1 ***Found Reservation***

1 key=key2 type=3

Press <ENTER> to continue ...
```

10. Again from the menu, choose **3** and make sure that it executes successfully.

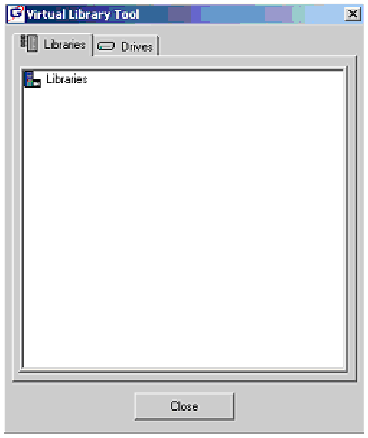
    If any of the above 3 commands do not execute successfully, check the inter-connecting hardware, such as storage routers or bridge, to see whether these commands are supported. (Refer to the hardware manufacturer's documentation to see if this operation is supported.)

```
1.Register    2.Reserve    3.Release
4.Clear       5,Prempt     6.Prempt And Abort
7.Register And Ignore Key

Please enter a service action? [1]: 2

1.Write Exclusive(0x01)    2.Exculsive(0x03)
3.Write Exclusive RO(0x05) 4.Exclusive RO(0x06)
5.Write Exclusive AR(0x07) 6.Exclusive AR(0x08)

Please enter a access type? [1]: 2

Please enter a registered key?: key3

Please enter a service action key?:

Executing the command...

Successful
```

VirtualLibrary Tool

USAGE NOTES

- The VirtualLibraryTool.exe file is located in the `<software installation path>\Base` folder. Recommend creating a shortcut on the desktop for the tool. The Virtual Library Tool's initial screen as shown in the sample image is displayed.
- Libraries created by the utility are actually XML files which are saved in the `<software installation path>\LibEmulator` folder.
- Virtual tape media can be created and imported from a `shelf` to a library. Virtual tape media can be exported back to a shelf, deleted, or moved to another library.
- Virtual tape will hold 40GB compressed. This capacity can be changed in the MMS2MediaType table.
- Virtual libraries DO NOT write backup data. Backups will run to a virtual library and report successful completion, however no actual data is written to virtual tape. As such, no data can be restored.
- Cleaning tapes are not supported in Virtual Libraries.
- Indexes created in the Index Cache directory can be used to browse the backup data list, but any attempt to restore data from virtual tape will fail
- The VirtualLibraryTool can create direct-attached (single MediaAgent), dynamic/SAN (multiple MediaAgent), and shared (split between multiple MediaAgent) libraries. Stand-alone libraries and pooled Standalone libraries can be configured using the Library and Drive Configuration tool or by directly editing the library xml file.

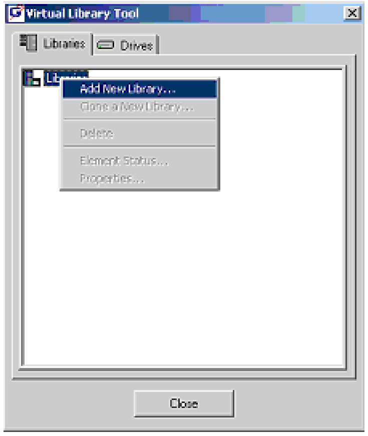


CREATING A DIRECT ATTACHED LIBRARY

Start the VirtualLibraryTool utility.

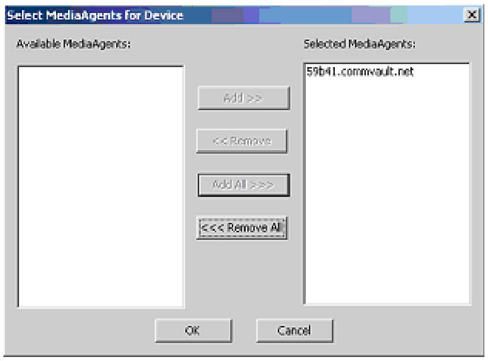
1. In the `Virtual Library Tool` window, right-click on the Libraries object level and select `Add New Library` from the shortcut menu

The Select MediaAgents for Device window will open.



2. In the `Select MediaAgents for Device` window, select the MediaAgent that will control the library.

Click `OK` to close the MediaAgent selection window and open the `Library Properties` window.



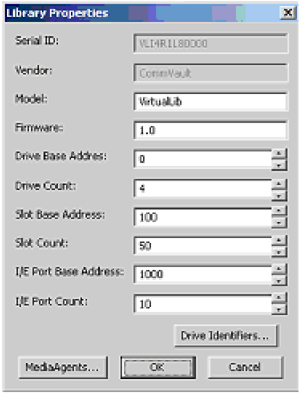
Available MediaAgents:

Selected MediaAgents: 59b41.commvault.net

3. In the Library Properties window, set the Drive Count, Slot Count, and I/E Port Count values. To emulate a specific vendor library, you can also set the Model and Firmware values.

Base Address values are for advanced use. Do not edit.

When you have set all values click on the Drive Identifiers button to open the Drive Identifiers window.



Serial ID: VLI4R1L80000

Vendor: CommVault

Model: VirtualLib

Firmware: 1.0

Drive Base Addres: 0

Drive Count: 4

Slot Base Address: 100

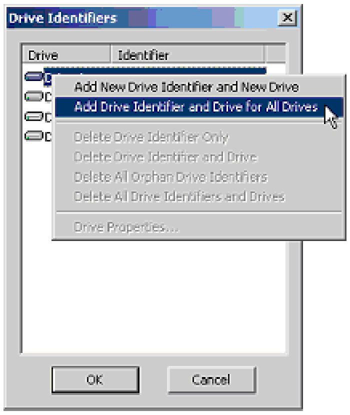
Slot Count: 50

I/E Port Base Address: 1000

I/E Port Count: 10

4. In the Drive Identifiers window, right-click on any drive and select the Add Drive Identifier and Drive for All Drives option.

The Select MediaAgents for Device window will open.

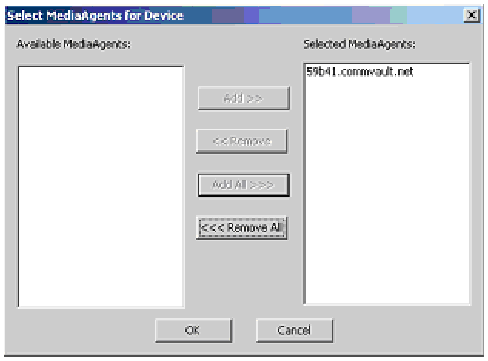

Drive Identifiers
Drive
Identifier
Add New Drive Identifier and New Drive
Add Drive Identifier and Drive for All Drives
Delete Drive Identifier Only
Delete Drive Identifier and Drive
Delete All Orphan Drive Identifiers
Delete All Drive Identifiers and Drives
Drive Properties...
OK
Cancel

5. In the Select MediaAgents for Device window, select the MediaAgent that will control all the drives.

Click OK to close the MediaAgent selection window.

Click OK to close the Drive Identifier window.

Click OK to close the Library Properties Window.



Available MediaAgents:

Selected MediaAgents: 59b41.commvault.net

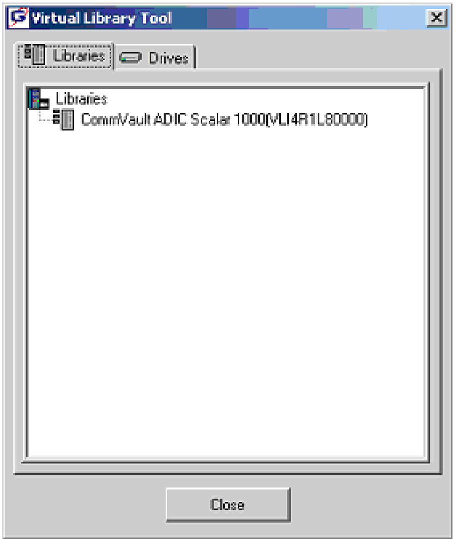
6. The newly created library should appear in the Libraries tab of the Virtual Library Tool window.

Click on the Drives tab and verify that the number of drives specified for that library are listed.

Both the library and all drives should have a serial number next to their description.

Click Close to exit the Virtual Library Tool.

You have successfully created a virtual tape library.

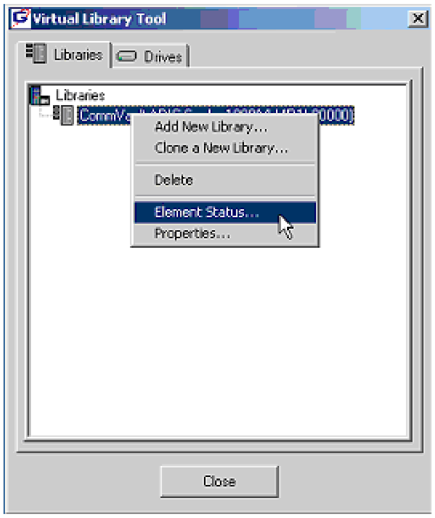


CREATING AND ADDING VIRTUAL TAPE TO A LIBRARY

Start the VirtualLibraryTool utility.

1. In the Virtual Library Tool window, right-click on the Libraries object level and select Element Status from the shortcut menu

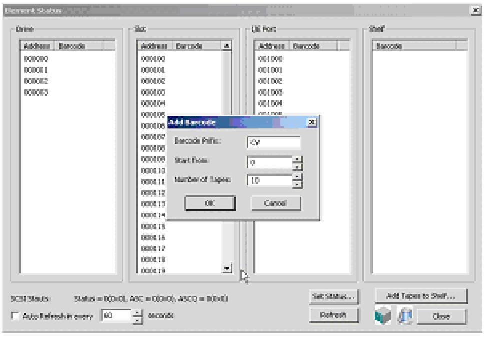
The Element Status window will open.



In the Element Status window, click on the Add tapes to Shelf button.

2. Enter a Barcode Prefix (optional); a starting barcode number; and the number of virtual tapes to create.

Click OK to create the tapes. The tapes will appear in the Shelf window on the right.



Barcode Prefix: CV

Start From: 0

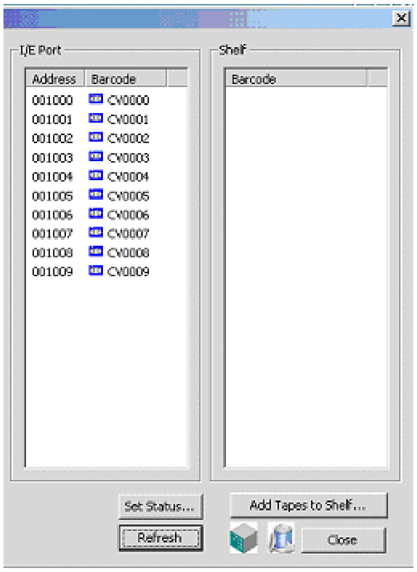
Number of Tapes: 10

3. Use the shift key and mouse, highlight the number of tapes in the Shelf window that you want to import.

DO NOT import more tapes then the number of I/E Ports available

DRAG the selected tapes into the I/E Port window or Slot Addresses

For configured libraries, tapes should move from the I/E ports into library slots within 30 seconds. Click the Refresh button or enable the Auto Refresh option and set the refresh interval.



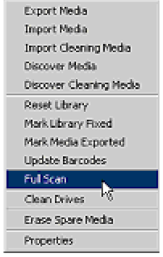
Address	Barcode
001000	CV0000
001001	CV0001
001002	CV0002
001003	CV0003
001004	CV0004
001005	CV0005
001006	CV0006
001007	CV0007
001008	CV0008
001009	CV0009

Barcode

Additional media can be added at anytime by repeating the above steps.

4. Do not duplicate barcodes.

Tapes will move from the I/E ports into library slots within 30 seconds. Click the `Refresh` button or enable the `Auto Refresh` option and set the refresh interval.

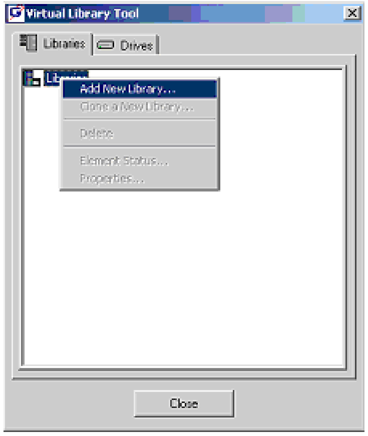


CREATING A SHARED TAPE LIBRARY

Start the VirtualLibraryTool utility.

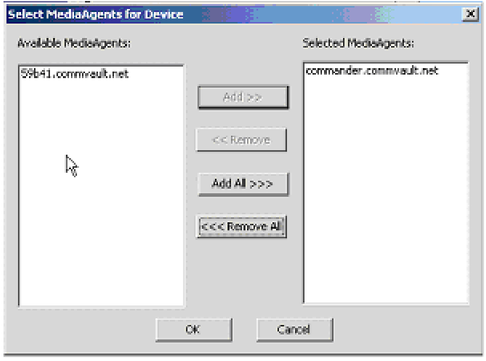
1. In the `Virtual Library Tool` window, right-click on the Libraries object level and select `Add New Library` from the shortcut menu

The `Select MediaAgents for Device` window will open.



2. In the `Select MediaAgents for Device` window, there should be at least two MediaAgents. Select the one MediaAgent that will control the library.

Click `OK` to close the MediaAgent selection window and open the `Library Properties` window.



Select MediaAgents for Device

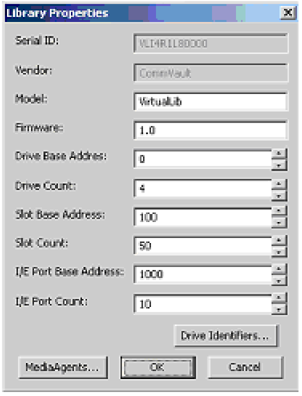
Available MediaAgents: 59b41.commvault.net

Selected MediaAgents: commander.commvault.net

3. In the `Library Properties` window, set the Drive Count, Slot Count, and I/E Port Count values. To emulate a specific vendor library, you can also set the Model and Firmware values.

Base Address values are for advanced use. Do not edit.

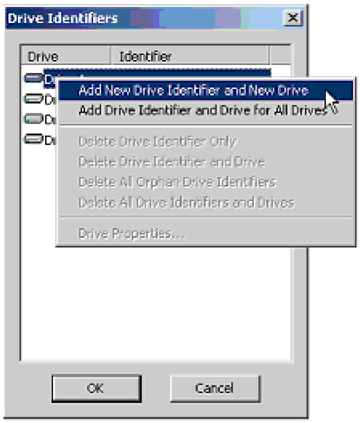
When you have set all values click on the `Drive Identifiers` button to open the `Drive Identifiers` window.


Library Properties

Serial ID: VLI4R1L80000
Vendor: CommVault
Model: VirtualLib
Firmware: 1.0
Drive Base Addres: 0
Drive Count: 4
Slot Base Address: 100
Slot Count: 50
I/E Port Base Address: 1000
I/E Port Count: 10

4. In the `Drive Identifiers` window, right-click on first drive and select the `Add New Drive Identifier and New Drive` option.

The `Select MediaAgents for Device` window will open.


Drive Identifiers
Drive
Identifier
Add New Drive Identifier and New Drive
Add Drive Identifier and Drive for All Drives
Delete Drive Identifier Only
Delete Drive Identifier and Drive
Delete All Orphan Drive Identifiers
Delete All Drive Identifiers and Drives
Drive Properties...
OK
Cancel

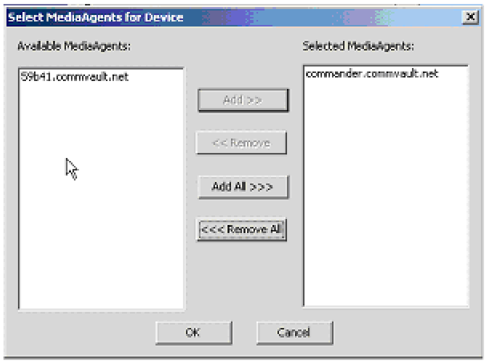
5. In the `Select MediaAgents for Device` window, select which one of the available MediaAgents will control that the drive.

Click `OK` to close the MediaAgent selection window.

Repeat steps 4 and 5 for each drive, selecting which one of the available MediaAgents will control each drive.

Click `OK` to close the Drive Identifier window.

Click `OK` to close the `Library Properties` Window.


Select MediaAgents for Device

Available MediaAgents: 59b41.commvault.net

Selected MediaAgents: commander.commvault.net

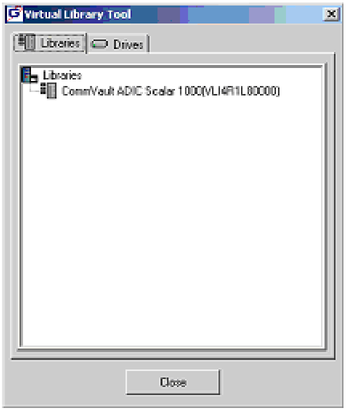
6. The newly created library should appear in the `Libraries` tab of the `Virtual Library Tool` window

Click on the `Drives` tab and verify that the number of drives specified for that library are listed.

Both the library and all drives should have a serial number next to their description.

Click `Close` to exit the Virtual Library Tool.

You have successfully created a shared virtual tape library.


Virtual Library Tool

Libraries
CommVault ADIC Scalar 1000(VLI4R1L80000)

CREATING A DYNAMIC/SAN TAPE LIBRARY

Follow all steps in the procedure for creating a direct-attached library except select all MediaAgents that will see the library and all the MediaAgents that will see the drives.

1.

CREATING A STAND-ALONE LIBRARY

OPTION 1

1. Follow all steps in the procedure for creating a direct-attached library. The Library should have at least 2 drives plus as many drives as you expect to make stand-alone libraries. You do not need to create media. Virtual stand-alone libraries will be automatically loaded with a virtual tape.
2. In the `Library and Drive Config` tool, right-click on a drive of the newly created library and select `Create Stand-alone Library`. Note that you can create many stand-alone libraries in this manner. However, there must be at least two drives left in the source library.
3. If you intend to pool the stand-alone libraries, do not configure them at this point.
4. Right-click on the library and configure the library and all drives.

OPTION 2

1. Follow all steps in the procedure for creating a direct-attached library. The Library should have 1 drive – no slots and no import/export mail slots. You do not need to create media. Virtual stand-alone libraries will be automatically loaded with a virtual tape.
2. Using notepad, open the `LibEmulator/<library>.xml` file. Look for the tag `<ScsiDeviceType>8</ScsiDeviceType>`. Change the 8 to a 4 and save the file.
3. In the `Library and Drive Config` tool, discover the new stand-alone library. Right-click on the library and configure the library and all drives.

CREATING A POOLED STAND-ALONE LIBRARY

1. See Creating a Stand-alone Library to create multiple stand-alone libraries.
2. If you used option 1 to create stand-alone libraries, use one un-configured stand-alone library as the target and drag the drive pool from each of the other un-configured stand-alone library into the target. Right-click and configure.
3. If you used option 2 to create stand-alone libraries, detecting the libraries should automatically pool them.

EXPORTING VIRTUAL TAPE

1. You can export virtual tapes using the standard export tasks or you can export using VaultTracker. Exported Media will appear in the I/E port, or, if using Virtual Mail slots, they will appear in the designated virtual mail slot(s) and range.
2. Open the VirtualLibraryTool; right-click on the library and select `Element Status`.
3. Locate the exported media; highlight; and drag to the shelf. The changed status will be reflected back to the CommCell Console within 30 seconds

MOVING VIRTUAL TAPE BETWEEN LIBRARY SHELVES

1. You can move virtual tapes from one library shelf to another.
2. Open the VirtualLibraryTool; right-click on the source library and select `Element Status`.
3. Select tapes on the shelf and drag them down to the Library Icon (cube shape icon next to Refresh button).
4. In the `Select Library` window that appears, select the target library. Click `OK`.
5. Close the `Element status` window; right-click on the target library; and select `Element Status`.

Disk Library Replication

Topics | How To | Related Topics

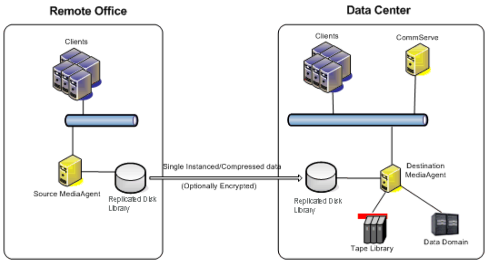
OVERVIEW

The Disk Library Replication solution is designed to seamlessly replicate data from remote offices to a centralized data center, where it is stored on disk media for ready access. Consolidating all backup data at the centralized data center provides redundancy for disaster recovery, as well as an alternate source for normal data recovery operations. This innovative solution is easily deployed, without any disruption of current data protection operations, and with no impact on your end users at remote offices; no additional software or configuration is required on client computers, as only MediaAgents are involved. Even more importantly, the data from every *i*DataAgent deployed at remote offices can be replicated to the centralized data center, no matter the source of the data -- all supported file systems, databases, and data types.

Significant benefits result when this solution is combined with several other available features; Deduplication performs deduplication at the remote office before data is replicated to the centralized data center, greatly reducing the network load; for information about MediaAgents and data types supported by deduplication, see Deduplication - Support. Replication Compression provides a similar benefit, compressing data at the remote office, replicating it across the network to the centralized data center, then uncompressing it on the destination MediaAgent; finally, Replication Encryption can be employed to ensure the security of data transmitted across non-secure networks, by encrypting the data before transmission and automatically decrypting it on the destination MediaAgent at the centralized data center.

A typical Disk Library Replication solution is shown in the illustration.

Software is deployed on a MediaAgent located at a remote office, and a MediaAgent located at the centralized data center. Thus, there is no impact on end users and client computers, since all operations involve MediaAgents only. Deployment and configuration occur once, and the solution continues to function without any further operator intervention. Once the initial transfer of data has been completed at the time of deployment, all data replication after that point will involve only data that has changed on the MediaAgent, similar in concept to Incremental Backups. This is different from an Auxiliary Copy operation, which is similar in concept to Full Backups, copying all selected data every time it runs, and also expanding all deduplicated data each time.



PRE-REQUISITES

The Disk Library Replication solution replicates data from one MediaAgent to another; typically, this would involve a MediaAgent installed in a remote office, and one installed at a centralized data center, although several remote office MediaAgents can replicate their data to the same centralized MediaAgent. Note that each remote MediaAgent will require a different mount path on the centralized MediaAgent.

Each MediaAgent computer requires the following:

- Meets System Requirements for both MediaAgent and ContinuousDataReplicator software. Disk Library Replication solution is also supported on Windows clustered computers.

  The platform on which the software is installed must be supported for both the MediaAgent and ContinuousDataReplicator software components.

- MediaAgent and ContinuousDataReplicator (CDR) software installed; see Installation.
- Shared Disk Library configured to use replicated disks on both source (remote office) and destination (centralized data center) MediaAgents; see Overview of Disk Libraries on Replicated Disks.

In addition, it is recommended that each MediaAgent have the following configured for this solution:

- Deduplication
- Replication Compression

- Replication Encryption (optional, when transmitting data across non-secure networks)

For a list of required product and feature licenses, see License Requirements.

HOW TO USE THE DISK LIBRARY REPLICATION SOLUTION

This section details how to deploy and configure, temporarily disable, or uninstall the Disk Library Replication solution.

INSTALL, CONFIGURE, AND BEGIN USING THE DISK LIBRARY REPLICATION SOLUTION

1. Install the latest version of the MediaAgent and ContinuousDataReplicator (CDR) software on a source (remote office) computer and destination (centralized data center) computer designated for this solution. For step-by-step instructions, see Installation.
2. Configure the Disk Libraries on Replicated Disks:
   - Using designated disks on the source and destination MediaAgents, Configure Disk Libraries on Replicated Disks; for general information, see Overview of Disk Libraries on Replicated Disks. In the Add Disk Library screen, select the **Enable Replication** option for the Shared Disk Device you just configured. Do not select the **Automatically create storage policy for new datapath** option if you plan to use Deduplication.

     When you have completed configuring the Disk Libraries on Replicated Disks, a Replication Set with the name "SimpleDataReplication" and associated Replication Pair(s) will be automatically created, and will appear in the CommCell Console under ContinuousDataReplicator on the source (remote office) MediaAgent. The Data Replication Type for the Replication Set will be set to Disk Library Replication option. For an example of how Replication Sets and Pairs appear in the Console, see Tree Levels in ContinuousDataReplicator. It is strongly recommended that you do not attempt to change any settings in the Properties of these automatically created Replication Sets and Pairs, except for those discussed in this section.
   - If you are using Disk Library Replication Solution on clusters, ensure that the Disk Library Replication option is selected in the Replication Set (Advanced tab) on all cluster nodes.
3. Create a Storage Policy to be used for this solution, using the Disk Library on Replicated Disks that you just configured; for general information, see Storage Policies. It is recommended that you also enable Deduplication of Data; for instructions, see Deduplication.
4. Configure Subclients (new or existing) with the content to be backed up and replicated to the centralized data center. Make sure to use the Storage Policy you created in the previous step, which will replicate the data to the Disk Library on Replicated Disks. For instructions, see Create a New Subclient; for more information, see Subclients.
5. Synchronization of data between the source and destination MediaAgents can be configured by scheduling the replication jobs at desired intervals using the job scheduler.

   Use the following steps to schedule the replication job:
   - From the CommCell Browser, navigate to **Client Computers** | ***<source_client_computer>***
   - Right-click the **Disk Library Replication**, point to **All Tasks** and then click **Backup**.
   - Select the desired **Backup Type**.
   - From the **Job Initiation**, click the **Schedule** option and then click **Configure** button.
   - Schedule the job as required, from the Schedule Details dialog box and then click **OK**. See Scheduling for more information.
   - Click **OK** to close the Backup Options dialog box.
6. Additional recommended options for this solution:
   - Enable Software Compression for a Replication Set; for more information see Replication Compression.
   - Configure the Replication Set for Data Encryption; for more information see Replication Encryption.
   - Configure Throttling for CDR Replication Activities; for more information see Data Replication - Throttling.
7. Once the installation and configuration is complete on both the source and destination MediaAgents, replication will begin within the update interval specified earlier in this procedure.

TEMPORARILY DISABLE AND RE-ENABLE THE DISK LIBRARY REPLICATION SOLUTION:

Disk Library Replication solution can be temporarily disabled/re-enabled using one of the following methods:

- Using the `nSuspendSDR` registry key, in the source machine.
  - To disable, create the `nSuspendSDR` registry key and set its Value to "1".
  - To re-enable, set the value of the `nSuspendSDR` registry key to "0" or remove the key.
- Disable any job schedules created for the Disk Library Replication solution.

UNINSTALL/DECONFIGURE THE DISK LIBRARY REPLICATION SOLUTION:

1. Stop (abort) replication activities; create the `nSuspendSDR` registry key (if it does not already exist) and set its Value to "1".
2. Delete the Storage Policy that was created for this solution. For instructions, see Delete a Standard Storage Policy.
3. Delete the Replication Pairs and Replication Sets that were automatically created when the Disk Libraries on Replicated Disks were created.

4. Delete any job schedules created for the Disk Library Replication solution.
5. Deconfigure the Disk Libraries on Replicated Disks that were configured on the source (remote office) and on the destination (centralized data center) MediaAgents. For instructions, see Deconfigure Libraries; for overview information, see Deconfiguring Libraries and Drives.

   > To leave the CDR software installed and use it to perform data replication, deselect the Disk Library Replication option in the Replication Set (Advanced tab) and select Continuous Replication for data replication type in the Replication Set (General tab). Cycle the Replication Service (CVRepSvc) on both the source and destination computers, and skip the next step. For more information about Services, see Services.

6. Uninstall ContinuousDataReplicator (CDR) software from both the source (remote office) and destination (centralized data center) MediaAgent computers. For more information, see Uninstalling ContinuousDataReplicator.

HOW TO RECOVER DISK LIBRARY REPLICATION DATA

Use the following method to recover data that was backed up from a remote office to a centralized data center.

Browse Data from the source client in the usual manner, but select the centralized MediaAgent from the **Use MediaAgent** list in the Browse Options window. Then Restore Backup Data to the original client at the remote office, or to a location of your choosing. This method might be best suited to cases where data is being recovered to a single computer, as opposed to many computers.

BEST PRACTICES

Review the following recommendations when deploying the Disk Library Replication solution:

- It is strongly recommended that you employ Deduplication and Replication Compression as part of this solution, as the benefits in reducing the size of data and speeding throughput across the network are significant.
- When this solution will involve data being transmitted across non-secure networks Replication Encryption is recommended to ensure data security.
- When Replication Compression is enabled, do not also enable Data Compression on the MediaAgent.
- When Replication Encryption is enabled, do not also enable Data Encryption on the MediaAgent.
- While it is possible to change the read-write access for mount paths associated with replicated disks, this should never be done for the Disk Libraries on Replicated Disks used for this solution.

CONSIDERATIONS AND NOTES

Review the following to gain a better understanding of how this solution operates:

- Replication Pairs will display a state of "Stopped" in the CommCell Console when not actively moving data. This is because the Pair will activate at the interval you specified in the **Media Management Configuration (Service Configuration)** Control Panel (or registry key `SDRPairStartIntervalMins`), replicate data transferring any new or changed data, then enter the "Stopped" state until the interval completes again.
- The software automatically creates filters to exclude the area of disk where the deduplication database is active on the source MediaAgent, so that data from this area is never replicated to the destination MediaAgent. In addition, filters are created to exclude temporary files from replication (`/**/*.tmp` in UNIX and `*.tmp` in Windows.)
- The option to automatically delete orphan files is specified when the Replication Set is created by the software; for more information on this subject, see Orphan Files.
- Locked files will not be replicated; once write activity has ended for a particular file, and it is no longer locked, it will be replicated to the destination at the next update interval. Any data in the process of being backed up to the source MediaAgent in the remote office will not be replicated to the centralized MediaAgent. This means that replicated data can only be restored successfully if the backup that they were a part of had completed before the most recent replication started. Any backups that completed before the start time of the latest replication as shown in the Data Replication Monitor will be restorable.
- Most of the features of ContinuousDataReplicator are not functional when it is deployed for this solution.
- The data from a source (remote office) MediaAgent cannot be replicated to multiple destinations (commonly referred to as "fan-out") using this solution.
- If you are using Auxiliary Copy to read data from the destination, then deferred copy settings must be enabled for the Auxiliary Copy, for the number of days required for the replication to be complete. See Auxiliary Copy with Deferred Copies for details.

LICENSE REQUIREMENTS

The following products and features mentioned in this solution require an available Product License or Feature License in the CommServe:

- MediaAgent
- ContinuousDataReplicator (CDR)
- Deduplication

- Disk Libraries
- Data Encryption

Review general license requirements included in License Administration. Also, View All Licenses provides step-by-step instructions on how to view the license information.

Back to Top

Disk Library Replication - How To

Topics | How To | Related Topics

CONFIGURE DISK LIBRARIES ON REPLICATED DISKS

The following procedure describes the steps involved in configuring a shared disk library with static mount paths.

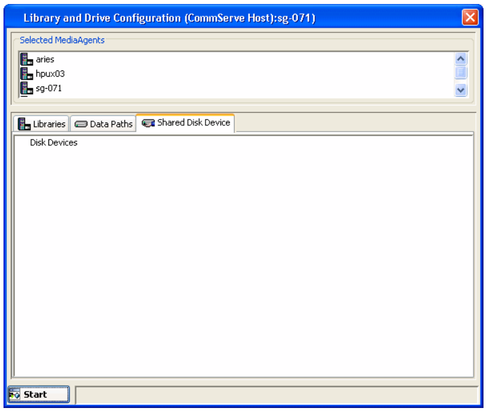
BEFORE YOU BEGIN

This feature requires a Feature License to be available in the CommServe® Server.

Review general license requirements included in License Administration. Also, View All Licenses provides step-by-step instructions on how to view the license information.

TO CONFIGURE DISK LIBRARIES ON REPLICATED DISKS

1. Display the Library and Drive Configuration window.
2. Click the **Shared Disk Device** tab.



Library and Drive Configuration (CommServe Host):sg-071)

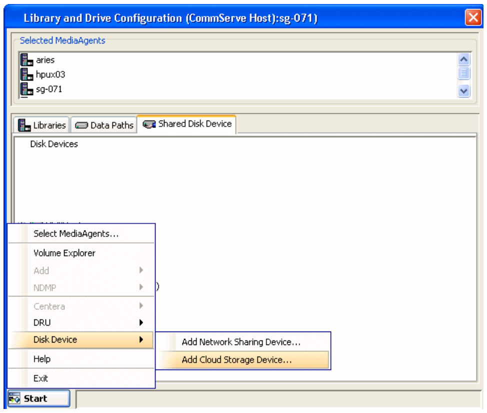
Selected MediaAgents

aries

hpux03

sg-071

3. Click the **Start** menu, select **Disk Device**, then choose **Add Network Sharing Device**.



4. In the **Add Sharing Folder** dialog box, enter/select the following information:

   MediaAgent - The name of the MediaAgent accessing the mount path.

   Folder - The network path that will be used by the MediaAgent to access the mount path

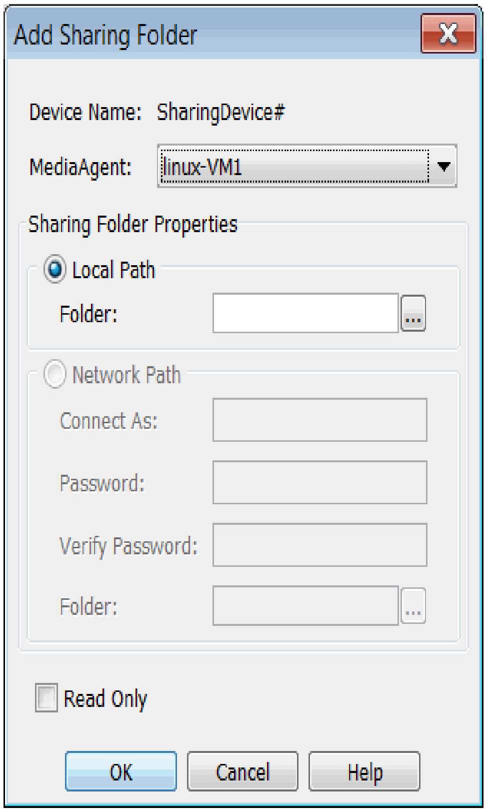
   If the MediaAgent is a Windows MediaAgent, you can choose a local path or a network path. If you use a network path provide the username and password that must be used by the system to access the device.

   NOTES:

   - Network path is not supported for Disk Library Replication solution; only local paths are supported.

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

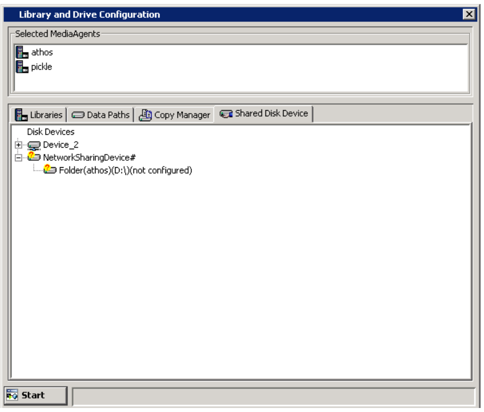
   Click **No** in the confirmation dialog box to add another sharing folder.



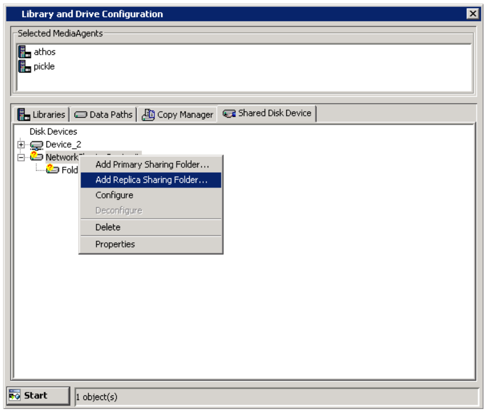
Device Name: SharingDevice#

MediaAgent: linux-VM1

The system displays the device information with the MediaAgent accessing the device in the **Library and Drive Configuration** window.



5. Right-click **NetworkSharingDevice** and then click **Add Replica Sharing Folder**.



6. In the **Add Sharing Folder** dialog box, enter/select the following information for the MediaAgent residing on the replica sharing folder.

MediaAgent - The name of the MediaAgent accessing the mount path.

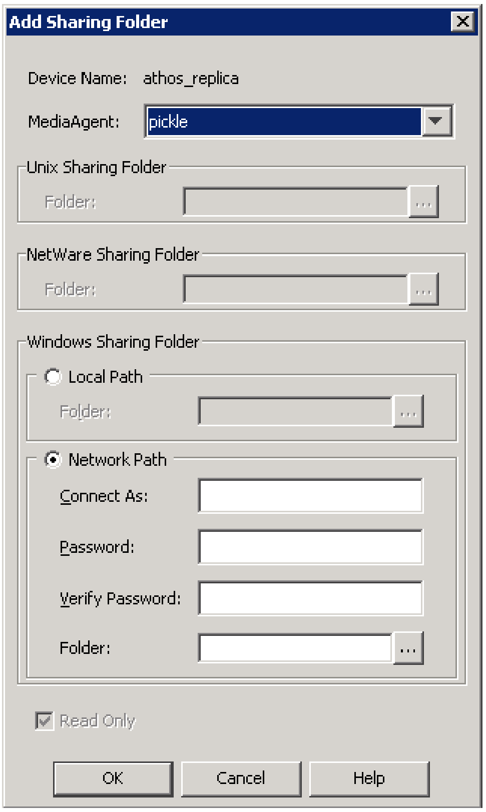
Folder - The path that will be used by the MediaAgent to access the mount path

If the MediaAgent is a Windows MediaAgent, you can choose a local path or a network path. If you use a network path provide the username and password that must be used by the system to access the device.

NOTES:

- Network path is not supported for Disk Library Replication solution; only local paths are supported.
- For Disk Library Replication solution, this is the destination sharing folder and cannot be the same as the sharing folder path given in Step 4.

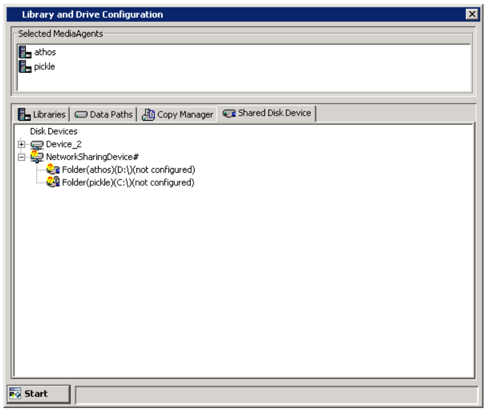
When you are finished, click **OK**.



Device Name: athos_replica

MediaAgent: pickle

The system displays the device information with the MediaAgent accessing the device in the **Library and Drive Configuration** window.

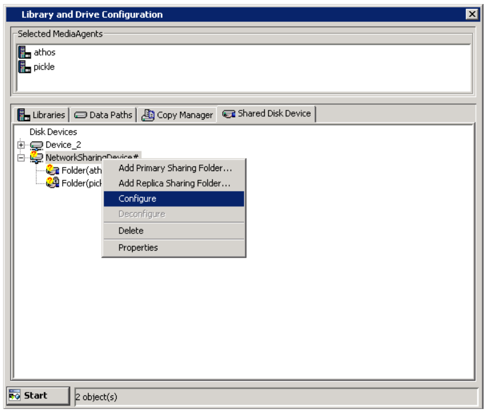


NetworkSharingDevice#

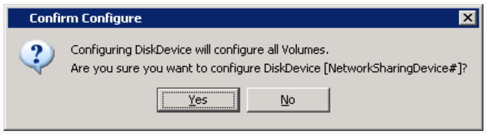
Folder(athos)(D:\)(not configured)

Folder(pickle)(C:\)(not configured)

7. Right-click **NetworkSharingDevice** and then click **Configure**.

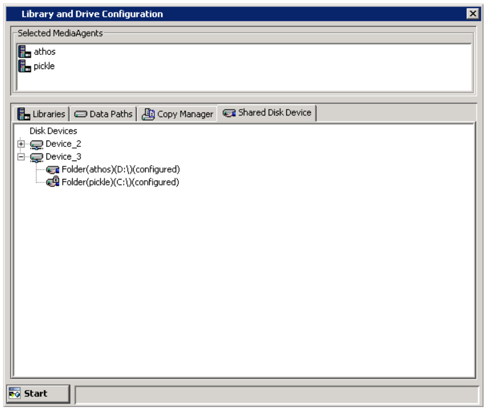


8. Click **Yes** to continue.



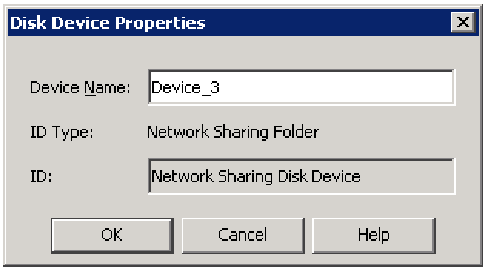
Configuring DiskDevice will configure all Volumes.
Are you sure you want to configure DiskDevice [NetworkSharingDevice#]?

The status of the folders changes to **configured** in the **Library and Drive Configuration** window.



9. Optionally rename the Device Name with an appropriate name, to avoid confusion.

To rename, right-click the device and then click **Properties**. In the **Device Properties** dialog box, type a new name.

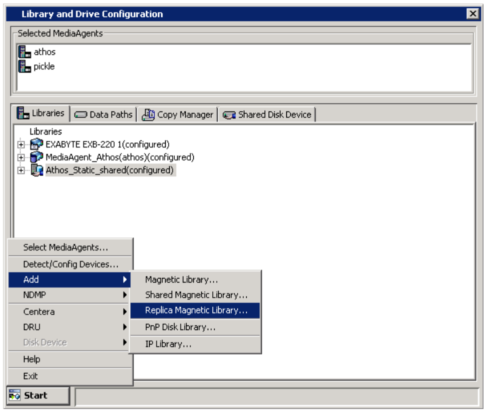


Device Name: Device_3

ID Type: Network Sharing Folder

ID: Network Sharing Disk Device

10. From the **General** tab of the **Library and Drive Configuration** window, click the **Start** menu, select **Add**, then choose **Replica Disk Library**.



11. In the **Add Disk Library** dialog box, enter the following:

Alias: A descriptive name for the disk library.

Automatically create storage policy for new data paths: Select this option to automatically create a new storage policy when the mount path is added to this disk library.

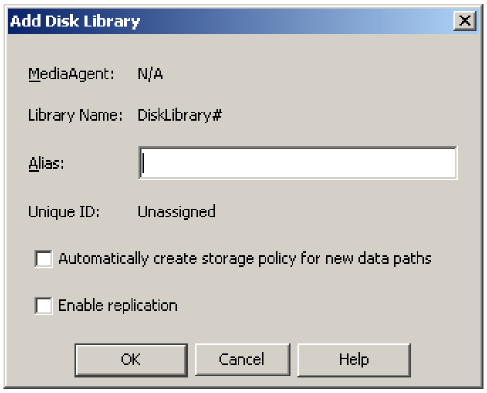
Enable Replication: For Disk Library Replication solution, select this option to use ContinuousDataReplicator to replicate data between the source (shared folder added in Step 4) and the destination (shared folder added in Step 6) mount paths. Leave this option unselected if you are using a third party application to replicate data between shared folders.

Selecting this option will automatically create a new replication set and a replication pair under ContinuousDataReplicator, when a mount path is added to this library. These replication sets and replication pairs can be monitored from the CommCell Console. It is highly recommended not to change the default settings of the replication sets, or delete the replication sets when the replication is in progress.

NOTES:

- If this option is selected, make sure to install the ContinuousDataReplicator package on the source and the destination computers before adding mount path to this library.

Click **OK**.



Add Disk Library

MediaAgent: N/A

Library Name: DiskLibrary#

Alias:

Unique ID: Unassigned

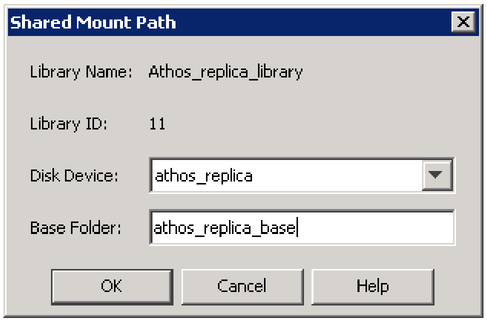
□ Automatically create storage policy for new data paths

□ Enable replication

12. In the **Shared Mount Path** dialog box, select the disk device that you wish to associate as the mount path from the **Disk Device** list.

    In the **Base Folder** box, type the name of the base folder under which the mount path can store data. Do not include the drive letter while adding the name of the base folder.

    Click **OK**.



Shared Mount Path

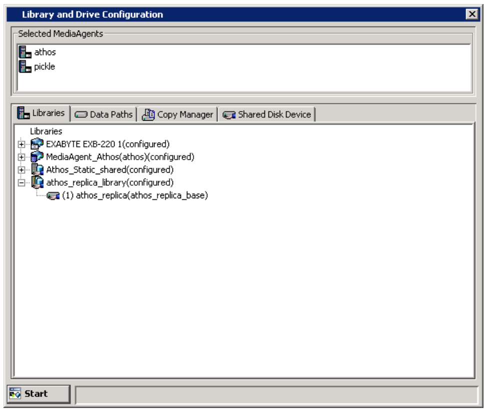
Library Name: Athos_replica_library

Library ID: 11

Disk Device: athos_replica

Base Folder: athos_replica_base

The disk library is configured.



Library and Drive Configuration

Selected MediaAgents

athos

pickle

Libraries

EXABYTE EXB-220 1(configured)

MediaAgent_Athos(athos)(configured)

Athos_Static_shared(configured)

athos_replica_library(configured)

(1) athos_replica(athos_replica_base)

Create a Storage Policy

Required Capability: See Capabilities and Permitted Actions

To create a storage policy:

1. From the CommCell Browser, right-click the Storage Policies node, and select New Storage Policy from the shortcut menu.
2. Follow the prompts displayed in the Storage Policy Wizard to configure the following:
    - Type of Storage Policy: `Backup`, `Compliance Archiver` or `Disaster Recovery Backup`
    - Name of Storage Policy (and Incremental Storage Policy, if selected)
    - Name of the Primary Copy
    - Name of the default library to which the Primary Copy should be associated
    - Name of the MediaAgent
    - Stream and Retention Configuration (default is infinite)
    - Designate Primary Copy for Deduplication: `Yes` or `No`. Also, select the Deduplication Type: `Block Level` or `Object Level`.

      If you wish to enable deduplication at the source, select the `Enable Client Side Deduplication` option.

        If you select `No`, you cannot enable deduplication on the primary copy at a later time. However, you can enable deduplication on the secondary copies during creation. See Enable Deduplication in a Secondary Copy for details.

   - Name of the Deduplication Store, MediaAgent for Deduplication Store access, and location of the Deduplication Database. If you wish to create a new deduplication store for the Storage Policy, then select `Create New Deduplication Store` and provide the location of the store. If you wish to deduplicate against an existing deduplication store from a different Storage Policy, then select `Use Existing Deduplication Store` and select the desired deduplication store from the list. Note that the deduplication database must be located in a folder and not directly under the root of a disk volume.

3. The **Review Summary** window is displayed. Review your selections and then click **Cancel**, **Back** (to return to a previous window to change a selection), or **Finish** (to exit and create the storage policy).

CREATE A NEW SUBCLIENT

Before You Begin

- Review Subclients.
- Do not create a subclient while the parent node or any sibling subclient has a data protection or archive operation currently running on it.
- In cases where a new subclient is created with the same name as a deleted subclient, the system will append a Unix time stamp to the deleted subclient's name in data protection job history reports and views to distinguish the two subclients. For example, *subclientname*_1104257351.
- Informix *i*DataAgents: If you will be using the Informix ONBAR utility to create backup and restore scripts, you need not create subclients. Otherwise, if you will be using the CommCell Console to back up and restore Informix database objects (subsets/dbspaces), then you will need to create a subclient.
- ProxyHost *i*DataAgents: If you are using a BCV, you must prepare a batch file or a shell script file on the backup host containing commands to synchronize and split the BCV. The Resource Pack includes information on configurations for these batch files or shell scripts, as well as examples that apply to specific applications and hardware (e.g., Exchange databases in an EMC Symmetrix environment). See Resource Pack for more information on the Resource Pack.

  The ProxyHost *i*DataAgent also requires that you set permissions for the batch/shell script file on the backup host.
- SQL Server Database *i*DataAgents: When running on Windows Server 2003 and VSS is enabled, the **New Subclient** command is not available.
- PostgreSQL *i*DataAgents: Once you configure the PostgreSQL instance, the system automatically generates the default backup sets and default subclients. However, you can use the CommCell Console to create user-defined subclients for dump backup sets to distribute some of the database content. You cannot create user-defined subclients for FS backup sets.

Required Capability: See Capabilities and Permitted Actions

To create a new subclient:

1. From the CommCell Browser, right-click the node (agent/backup set/archive set/instance) for which you want to create a new subclient, click **All Tasks** (if applicable), and then simply click **New Subclient** for most agents.
   - For the SQL Server *i*DataAgent, expand **New Subclient** and click either **Database** to include individual databases or **File/File Group** to include database elements**.**
2. Click the General tab or General (Quick Recovery Agent) tab of the Subclient Properties dialog box and type the name (up to 32 characters) of the subclient that you want to create.
   - For supported agents identified in Support Information - Snapshot Engines, you can select a QSnap option to snap data and then perform a data protection operation on the data.
   - For Image Level on Unix and Image Level ProxyHost on Unix, use the **Incremental Support Using** field to configure either a CXBF subclient or a checksum subclient and to enable incremental support for either subclient type.
   - For QR Agents, you must also select a QR Policy from the **QR Policy** list.
   - For the Windows *i*DataAgents that support VSS, you can optionally Enable VSS on a Subclient.
3. Select other options from the General tab as appropriate for the agent.
4. Click the **Content** or **Databases** tab of the Subclient Properties dialog box and Configure Subclient Content as appropriate for your agent.
5. For all agents (except QR), click the Storage Device (Data Storage Policy) tab of the Subclient Properties dialog box, then select a data storage policy to associate with this subclient from the storage policy list.
   - For the DB2 and DB2 DPF *i*DataAgents, you can also change the number of data backup streams. For the DB2 DPF *i*DataAgent, the default stream threshold should be equal to the total number of database partitions for the subclient.
   - For SQL Server *i*DataAgents, you can also click the Storage Device (Log Storage Policy) tab of the Subclient Properties dialog box, then select a log storage policy to associate with this subclient from the storage policy list and select the number of backup streams for transaction log backup jobs.
   - For 1-Touch for Unix, it is strongly recommended that the storage policy that you select for the subclient configured for 1-Touch use a MediaAgent on a different computer. If you do this, and if the system crashes, the media will not have to be exported to another MediaAgent in order to recover the system.
6. For Oracle and DB2 *i*DataAgents, click the Backup Arguments (Oracle) or Backup Arguments (DB2, DB2 DPF) tab of the Subclient Properties dialog box and Configure Backup Arguments as appropriate for your agent. Note that the backup arguments for Informix are located on the Content tab.
7. For Migration Archiver Agents, click the **Archiving Rules** or **Rules** tab of the Subclient Properties dialog box and configure archiving rules as appropriate

for your agent. In order to perform rules-based migration archiving operations, the **Disable All Rules** checkbox must be cleared.

If the File Archiver for Windows supports Data Classification, several filter-like configuration fields are defined as archiving rules and are available from the Subclient Properties (Rules) tab. If you want to define content and archiving rules based on file attributes other than volumes, size, and modified time (i.e., if you want to customize your rules), click the Advanced tab and configure as appropriate. Also, stub management options can be configured from the Stub Rule tab. See Configure Archiving Rules - File Archiver Agents for step-by-step instructions.

8. For ProxyHost and Image Level ProxyHost *i*DataAgents, click the Pre/Post Process tab of the Subclient Properties dialog box. In the **PreScan** field, type the path to the batch file/shell script file that contains those commands that are to run before each backup of the subclient, or click **Browse** to locate and select this file. For ProxyHost and Image Level ProxyHost, the file must reside on the backup host or primary host.
9. Optionally (if supported for your agent) you can:
   - Add a Data Protection or Discovery Filter for a Subclient on the Filters tab.
   - Configure a Subclient for Pre/Post Processing of Data Protection/Archive Operations on the Pre/Post Process tab.
   - Enable Software Compression for a Subclient on the Software Compression tab of the **Storage Device** tab.
   - Configure the Subclient for Data Encryption on the Encryption tab.
   - Enable or Disable Operations for this subclient on the Activity Control tab.
   - Configure Mailbox Stores for Auto-Discovery on the Auto-discovery tab.
   - Configure the Subclient for 1-Touch on the 1-Touch Recovery tab.
   - View or change the user group security associations for this subclient from the Security tab.
   - Determine location from where archive logs will be backed up or deleted from the Log Destinations tab.
10. Click **OK** to save the subclient configuration. For QR Agents, this procedure is now complete. For all other agents, continue on to the next step.
11. The Backup Schedule dialog box advises you to schedule data protection operations for your new subclient. It is recommended you elect to set a schedule now. You can also associate this subclient with an All Agent Types schedule policy (which is automatically created by the system, or can be a user defined Data Protection schedule policy). If you have already associated a schedule policy at a previous level (Backup Set/Instance, Agent, Client, or Client Computer Group) the schedules defined in the Schedule Policy will be automatically applied to the new subclient. See Schedule Policy for more information.
    - If you want to associate this subclient with an All Agent Types schedule policy, click **Associate with Generic Schedule Policy**, and then select that schedule policy from the drop-down list box. Click **OK**.
    - If you want to associate this subclient with a specific schedule policy, click **Associate to schedule policy**, and then select the schedule policy from the drop-down list box. Click **OK**.
    - If you have selected to define a schedule for this subclient:
      - Click **Schedule**.
      - From the Backup/Archive Options dialog box, select the type of data protection operation that you want to schedule.
      - If you want to set Advanced Backup/Archive Options, click **Advanced**.
      - After selecting the data protection type and any advanced options, click **OK**. The **Schedule Details** dialog box appears.
      - From the Schedule Details tab, select the scheduling options that you want to apply, then click **OK**.
    - If you don't want to create a data protection schedule at this time, click **Do Not Schedule,** and then click **OK**.

This task is now complete.

ENABLE OR DISABLE SOFTWARE COMPRESSION FOR A REPLICATION SET

Before you Begin

- Compression settings made at the Replication Set level are for compression of data between the source computer and the destination computer.

Required Capability: Capabilities and Permitted Actions

➨ To enable/disable software compression for a Replication Set:

1. From the CommCell Browser, right-click the Replication Set and select **Properties**.
2. From the Replication Set Properties (Replication Options) tab, either select or clear **Compression ON**.
3. Click **OK** to save your settings and close the Replication Set Properties.

CONFIGURE THE REPLICATION SET FOR DATA ENCRYPTION

Before You Begin

- Encryption settings made at the Replication Set level are for encryption of data between the source machine and the destination machine.

- Encryption must be enabled at the client level prior to configuring data encryption for a Replication Set residing on that client. See Configure the Client for Data Encryption.

Required Capability: Capabilities and Permitted Actions

To configure data encryption for a Replication Set:

1. From the CommCell Browser, right-click the Replication Set and select **Properties**.
2. From the Replication Set Properties (Replication Options) tab, either select or clear **Encrypt During Data Transfer**.
3. Click **OK** to save your settings and close the Replication Set Properties.

CONFIGURE THROTTLING FOR CDR REPLICATION ACTIVITIES

Before you Begin

- Review Throttling.

Required Capability: Capabilities and Permitted Actions

To configure throttling for CDR replication activities:

1. In the CommCell Browser, right-click the ContinuousDataReplicator icon of the source machine, and select **Properties**.
2. In the Operational Parameters tab of the CDR Properties screen, specify any of the following:

   Destination Computer: (On Windows only)

   - Minimum percentage of free disk space for log files, below which the rate at which log files are sent from the source machine(s) is throttled. This throttling will reduce the maximum transfer rate specified in **Throttling Amount** by 50%. If you do not specify a value in **Throttling Amount**, no throttling will be imposed.
   - Minimum percentage of free disk space for log files, below which to stop the source machine(s) from sending more log files.

   Source Computer:

   - On Windows, the minimum percentage of free disk space for log files, below which data replication is aborted.
   - Throttling Amount - maximum network transfer rate in megabits per second (Mbps). The Utilization Percentage specified in the **Edit Throttling Rule** dialog will be a percentage of the number entered here.
   - Bandwidth Throttling Rules - click **Add** to configure the following in the **Edit Throttling Rule** dialog:

     Days of Week

     Start time

     End time

     Utilization Percentage - based on the specified Throttling Amount (see previous item)
3. Click **OK** to save your changes.

Back to Top

Seeding a Deduplicated Storage Policy

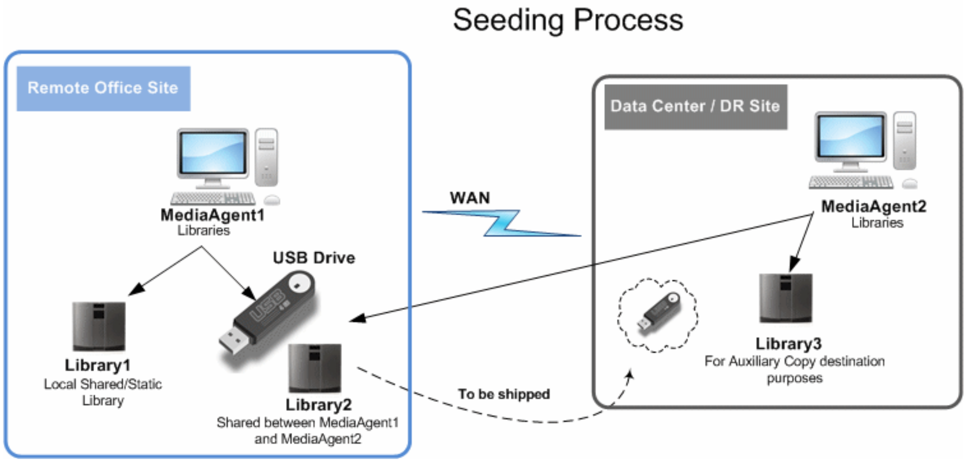
TABLE OF CONTENT

OVERVIEW

Data transfers across a high latency networks such as Wide Area Networks (WAN) can be time consuming, especially during the transfer of baseline backups where most of the data is unique and needs to be transferred.

The process in this section explains how to manually transfer baseline backup between two sites using easily available removable disks such as USB disks. As a part of this process, a pre-seeded source side deduplication database is created that is used to lookup signatures locally instead of across the network, thereby speeding up signature lookup operation and hence improving the overall data transfer speed.

This is useful in scenarios where remote office sites are separated from the data center across WAN and data either needs to be remotely backed up or periodically replicated to central data center sites. Once the initial baseline is established, all subsequent backup and Auxiliary Copy operations consume less network bandwidth as only the changes are transferred.



The diagram above represents the initial setup for the seeding to work.

HOW IT WORKS?

Storage Policy is configured to point to three copies - Primary, Secondary and Tertiary Copies.

- Primary copy points to local Disk Library at Remote Office site.
- Secondary copy is a temporary copy that points to a USB drive and is used to facilitate the transfer of baseline data to Data Center site.
- Tertiary copy points to local Disk Library at Data Center site.

Seeding process works as follows:

- At Remote Office site, data is first backed up to primary copy.
- Data is copied to secondary copy through Auxiliary Copy operation (on USB disks) and the USB disks are physically shipped over to Data Centers.
- Data is then copied from secondary copy (represented by USB disks) to tertiary copies through Auxiliary Copy operation.

  On Data Center MediaAgent, a `UseCacheDB` registry key is created to create Source Side Deduplication database prior to Auxiliary Copy operation.
- After copy of data, the source side deduplication database is manually copied from Destination MediaAgent to Source MediaAgent.

  The `UseCacheDB` registry key is created on the Source MediaAgent.
- Once the baseline is established, secondary copy is no longer required and is deleted. The source for tertiary copy will be modified to primary copy.

PREREQUISITES

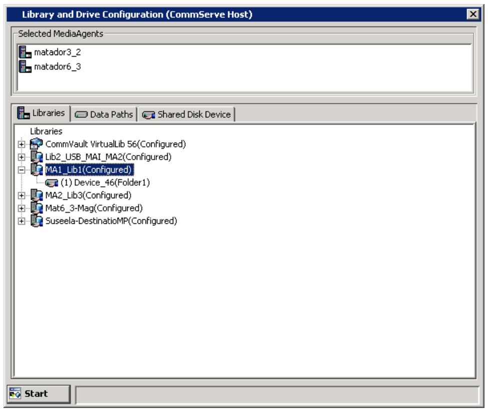
You should have the following setup configuration:

COMPONENTS

EXAMPLE

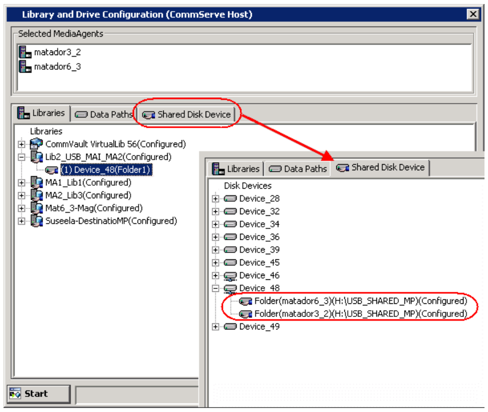
1. Configure a **Local Shared Library** (Library1), on MediaAgent1 computer located in the Remote Office Site.

   In the screenshot displayed on right, **matador6_3** is the MediaAgent1 at Remote Office site and **MA1_Lib1** is Library1.

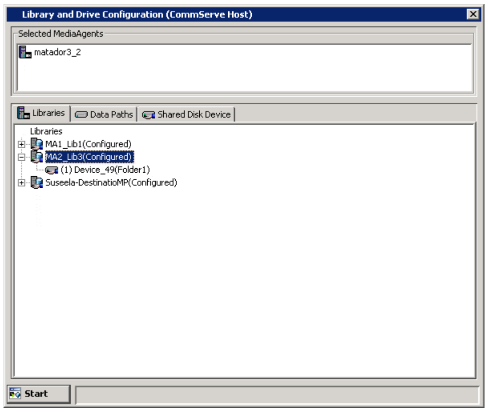


2. Configure a **Shared Library** (Library2), between MediaAgent1 and MediaAgent2 computers, on USB drive connected in the remote office site.

   In the screenshot displayed on right, MediaAgent1 is **matador6_3**, MediaAgent2 is **matador3_2** and Shared Disk Library is **Lib2_USB_MA1_MA2**.



3. Configure **Local Library** (Library3), used for Auxiliary Copy operation on MediaAgent2 computer located in the Data Center site.



CONFIGURATION

Pre-configure your setup with the following steps that involves the creation of a new storage policy and copies:

1. Create a **new storage policy** on MediaAgent1 computer and specify Library1 as the library to which the Primary Copy (Copy1) should be associated.

   - From the CommCell Console, navigate to **Policies**, right-click the **Storage Policies** node and click **New Storage Policy.**
   - Follow the prompts displayed in the Storage Policy Wizard.

     During creation, in the **Do you Want to enable Deduplication for primary copy?** dialog box, make sure **Deduplication** is selected and then click **Next.**

2.. Create a **Secondary Copy** (Copy2) on MediaAgent1 computer and specify Library2 as the library to which the Secondary copy should be associated.

   - Right-click the storage policy just created and click **All Tasks** | **Create Copy.**
   - Specify ***<Library2>*** as the library and ***<MediaAgent1>*** as the MediaAgent for the **Default Destination**.
   - Select **Deduplication** check box.
   - Click **OK**.

3. Create a **Tertiary Copy** (Copy3) on MediaAgent2 computer and specify Library3 as the library to which Tertiary copy should be associated.

- Right-click the storage policy and click **All Tasks** | **Create Copy.**
- Specify ***<Library3>*** as the library and ***<MediaAgent2>*** as the MediaAgent for the **Default Destination**.
- Select the **Enable Deduplication** check box.
- Click **OK**.

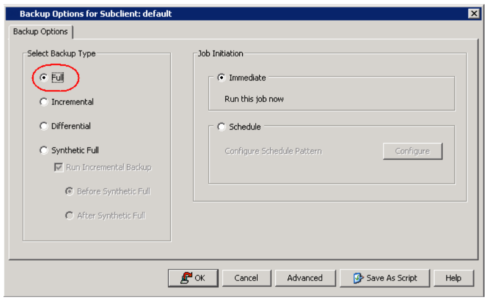
PERFORM SEEDING

The following steps explain how to perform the seeding process:

1. Perform the backups on all the clients associated with the Storage Policy.

   Use the following steps to perform the backup:

   - From the CommCell Console, navigate to **Client Computers** | **<MediaAgent1>**, right-click the **Subclient** and click **Backup**.
   - Select **Full** as backup type.
   - Click **OK**.


Backup Options for Subclient: default

Backup Options

Select Backup Type
● Full
○ Incremental
○ Differential
○ Synthetic Full
☑ Run Incremental Backup
● Before Synthetic Full
○ After Synthetic Full

Job Initiation
● Immediate
Run this job now
○ Schedule
Configure Schedule Pattern

2. Perform Auxiliary Copy to copy all the jobs from Primary Copy (Copy1) to Secondary Copy (Copy2).

Use the following steps to run the Auxiliary Copy:

a. From the CommCell Browser, navigate to **Policies | Storage Policies**.

b. Right-click ***<Storage_Policy>***, point to **All Tasks** and then click **Run Auxiliary Copy**.

c. Click **OK**.

The backup data is transferred to the USB drive and to the local drive (`Copy2`) on the Remote office site.

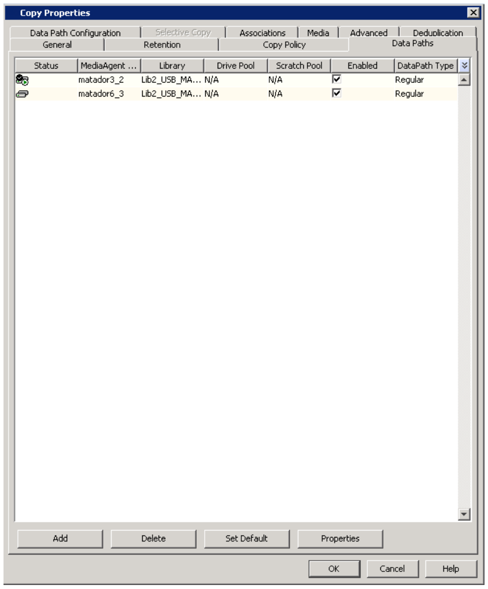
3. After completion of data copy, unplug the USB drive and ship it to the data center.

   Once the USB disks is available at the data center, plug the USB, and perform the following:

   - Navigate to **Policies** | **Storage Policies**, right-click the **<secondary copy>** and click **Properties.**
   - Click the **Data Path** tab.

     You should see Library2 enabled on both MediaAgent1 and MediaAgent2 computers.

     Once you unplug the USB drive on Remote Office, Library2 on MediaAgent1 will be offline.


Copy Properties

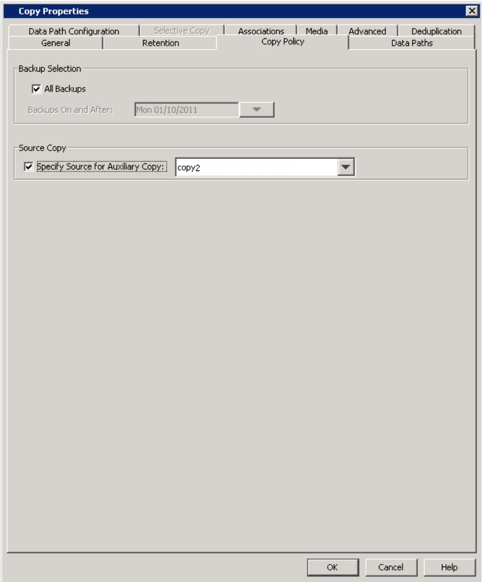
Status	MediaAgent ...	Library	Drive Pool	Scratch Pool	Enabled	DataPath Type
	matador3_2	Lib2_USB_MA...	N/A	N/A	☑	Regular
	matador6_3	Lib2_USB_MA...	N/A	N/A	☑	Regular

4. Create the registry key `UseCacheDB` on MediaAgent2 (Data Center site) computer.

   This registry key will create a source side Deduplication database that will be seeded with signatures during the Auxiliary Copy process.

See Managing Registry Keys from the CommCell Console for more information.

5. Associate Secondary Copy as a Source Copy for the Tertiary Copy.
   - Right-click the **<tertiary copy>** and click **Properties.**
   - Click the **Copy Policy tab.**
   - Under **Source Copy**, select Specify **Source for Auxiliary Copy** check box, and select **Secondary Copy** from the list.



Backup Selection

☑ All Backups

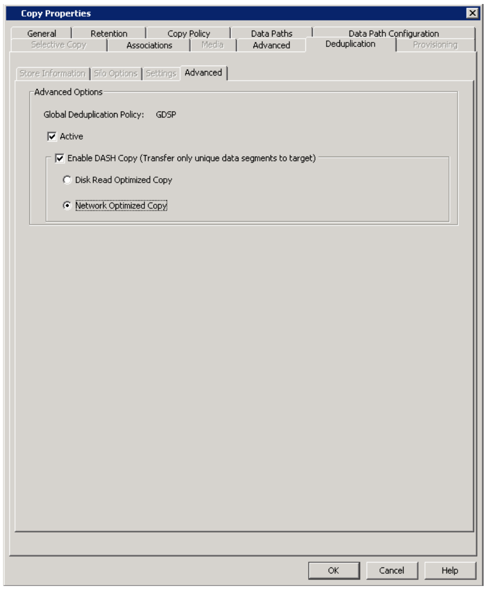
Backups On and After: Mon 01/10/2011

Source Copy

☑ Specify Source for Auxiliary Copy: copy2

6.. Enable **DASH copy** on the Tertiary Copy.

- Right-click the ***<tertiary copy>*** (Copy3) and click **Properties**.
- Click the **Deduplication** tab, then the **Advanced** tab.
- Click **Enable DASH Copy** and select **Network Optimized Copy**.
- Click **OK**.



Advanced Options

Global Deduplication Policy: GDSP

☑ Active

☑ Enable DASH Copy (Transfer only unique data segments to target)

○ Disk Read Optimized Copy

● Network Optimized Copy

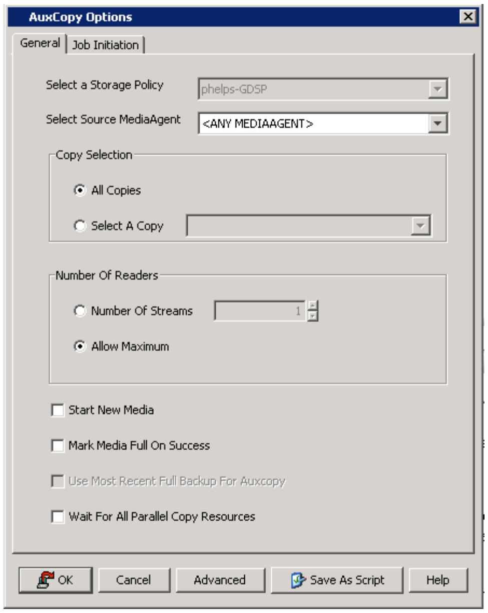
7.

- From the CommCell Console, navigate to **Policies** | **Storage Policies**.
- Right-click your **<storage policy>** and click **All Tasks | Run Auxiliary Copy.**

  Auxiliary copy jobs should not be run from the Remote office site until the source side database is copied from MediaAgent2 to MediaAgent1 computer after seeding.

- Click **OK**.

  This will seed the deduplication policy and will create a source side deduplication database on MediaAgent2 computer under the job results folder.



AuxCopy Options

General | Job Initiation

Select a Storage Policy: phelps-GDSP

Select Source MediaAgent: <ANY MEDIAAGENT>

Copy Selection

● All Copies

○ Select A Copy

Number Of Readers

○ Number Of Streams: 1

● Allow Maximum

□ Start New Media

□ Mark Media Full On Success

□ Use Most Recent Full Backup For Auxcopy

□ Wait For All Parallel Copy Resources

8. Manually copy the seeded source side database from the Job Results folder of MediaAgent2 back to MediaAgent1.

If Global Deduplication Policy is being used and there are multiple policies pointing to the same GDSP policy, you must copy the seeded database from the Job Results folder of each computer to the respective MediaAgent(s) Job Results source folder.

EXAMPLE

Copy `CV_CLDB_AUX_98` from the Job Results folder of MediaAgent2 to the Job Results folder of MediaAgent1:

```
C:\<software>\iDataAgent\JobResults\CV_CLDB\
CV_CLDB_AUX_98
```

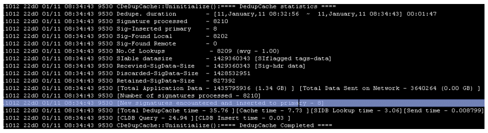
9. Delete the seeded database from the Job Results folder of MediaAgent2.

10. After seeding process, re-associate primary copy as source copy for Tertiary Copy.

- Right-click ***<tertiary copy>*** (Copy3) and then click Properties.
- Click the **Copy Policy** tab.
- Clear **Source Copy** check box to use **Copy1** (primary copy) as source copy during Auxiliary Copy operation.
- Delete secondary copy as this is no longer needed.

11. Run a full backup followed by an Auxiliary Copy job.

You will see a minimum amount of data being transferred between MediaAgent1 and MediaAgent2. Any backup or auxiliary copies started at the remote office site will now verify data signatures from the seeded source side deduplication database. If a signature is already present in the source side deduplication database this means the data block is already available at the data center and will not be transferred.



```
1012 22d0 01/11 08:34:43 9530 CDeDupCache::Uninitialize():==== DedupCache statistics ====
1012 22d0 01/11 08:34:43 9530 Dedupe. duration        - [11,January,11 08:32:56  ~  11,January,11 08:34:43] 00:01:47
1012 22d0 01/11 08:34:43 9530 Signature processed     - 8210
1012 22d0 01/11 08:34:43 9530 Sig-Inserted primary    - 8
1012 22d0 01/11 08:34:43 9530 Sig-Found Local         - 8202
1012 22d0 01/11 08:34:43 9530 Sig-Found Remote        - 0
1012 22d0 01/11 08:34:43 9530 No.Of Lookups            - 8209 (avg - 1.00)
1012 22d0 01/11 08:34:43 9530 SIable datasize         - 1429360343 [SIflagged tags-data]
1012 22d0 01/11 08:34:43 9530 Recevied-SigData-Size   - 1429360343 [Sig-hdr data]
1012 22d0 01/11 08:34:43 9530 Discarded-SigData-Size  - 1428532951
1012 22d0 01/11 08:34:43 9530 Retained-SigData-Size   - 827392
1012 22d0 01/11 08:34:43 9530 [Total Application Data - 1435795936 (1.34 GB) ] [Total Data Sent on Network - 3640264 (0.00 GB) ]
1012 22d0 01/11 08:34:43 9530 [Number of signatures processed - 8210]
1012 22d0 01/11 08:34:43 9530 [New signatures encountered and inserted to primary - 8]
1012 22d0 01/11 08:34:43 9530 [Total DedupCache time - 35.76 ][Cache time - 7.73 ][SIDB Lookup time - 3.06][Send time - 0.008799]
1012 22d0 01/11 08:34:43 9530 [CLDB Query - 24.94 ][CLDB Insert time - 0.03 ]
1012 22d0 01/11 08:34:43 9530 CDeDupCache::Uninitialize():==== DedupCache Completed ====
```