Administration Guide - Unix File Archiver Agent

TABLE OF CONTENTS

Overview - Unix File Archiver Agent

TABLE OF CONTENTS

INTRODUCTION

File Archiver for Unix Agent is installed as a stand alone archiving agent, and is not dependent on the Unix File System iDataAgent.

The Archived data allows preservation, transparent retrieval, and discovery of information held within file system environment. It reduces the size of data on the primary storage and decreases the duration of backup operations by the corresponding iDataAgent. Migrating data from file systems to secondary, tiered-storage maximizes storage utilization across the enterprise.

The File Archiver for Unix can optionally create stubs that contain information about the archived data to facilitate end-users with non-browse recovery operations from third-party applications. Migrated data can also be recovered from the CommCell Console using the browse recovery operation whether the stubbing feature is enabled or disabled. Additionally, it employs centralized, policy-based storage to reduce costs and simplify management.

KEY FEATURES

The Unix File Archiver involves the following key features:

RECALL THROTTLING

You can configure the stub recovery parameters, such that, you can set the Maximum Number of Stubs in a Recall Job, Time between recalls and Time to wait after maximum successive recalls limit is reached.

POINT IN TIME RESTORE

You can restore the system state of a client, backed up on a specific date and time.

STUB PRUNING

In the archive phase, File Archiver for Unix will archive files meeting the pre-set archive criteria and, if applicable, put them into a list for the stubbing phase and prune the expired stubs. This helps in secondary storage space reclamation.

TERMINOLOGY

The Unix File Archiver documentation uses the following terminology:

MIGRATION ARCHIVING	Migration archiving is a process of periodically moving unused or infrequently used Unix File System data on a host computer to secondary storage, thereby reducing the size of data on the primary storage.
STUBBING	The stubbing phase starts after the archive phase succeeds. Stubs are placeholders of the original data after it has been migrated to the secondary storage. Stubs replace the archived files in the location selected by the user during the archive. However, stubs will only be created if the subclient properties were configured to create them during archive.
DATA RECOVERY	The archived and migrated data can be recovered in any of the following three methods: ● Recovery of archived files per file paths provided using the CommCell Console. ● Browse and Recovery of archived files using the CommCell Console. ● Recall of archived files from stubs using third-party applications like: Unix Terminal or Console window.
STUB RECOVERY	If the subclient is configured to create stubs, you can perform a recall operation from a Unix workstation for recovering the stubs. A recall is any action that causes an open and read to be executed on the stub, which automatically initiates a recovery operation.

System Requirements - File Archiver for Unix Agent

System Requirements | Supported Features | Supported File Systems

The following requirements are for the File Archiver for Unix Agent and Add-On Archiver Agent:

OPERATING SYSTEM		PROCESSOR
AIX	AIX 7.1	Power PC (Includes IBM System p)
	AIX 6.1 64-bit	Power PC (Includes IBM System p)
	AIX 5.3 32-bit and 64-bit with technology level 7 (or higher) and runtime library xlC.rte 8.0.0.0 or higher Note that all AIX platforms support Logical Partitions (LPAR).	Power PC (Includes IBM System p)
HP-UX	HP-UX 11.31 64-bit	Itanium
	HP-UX 11.31 64-bit	PA-RISC
	HP-UX 11.23 64-bit	PA-RISC
	HP-UX 11.23 64-bit	Itanium
LINUX	**CENTOS**	
	CentOS 5.4 with kernel 2.6.18-164	Intel Pentium or compatible minimum required
	CentOS 5.3 with kernel 2.6.18-128	Intel Pentium or compatible minimum required
	DEBIAN	
	Debian 5.x with kernel 2.6.26-2	Intel Pentium or compatible minimum required
	Debian 5.x with kernel 2.6.26.19-2	x64
	OES LINUX	
	Novell OES2 Linux up to SP2 (SLES 10 SP2) 64-bit In order to perform a stub recall from Linux OES NSS volumes, Linux OES File System iDataAgent must be installed.	x64
	Novell OES2 Linux up to SP2 (SLES 10 SP2) 32-bit	Intel Pentium or compatible minimum required
	RED HAT ENTERPRISE LINUX	
	Red Hat Enterprise Linux AS 4.9 with kernel 2.6.9-100 (Update 9)	Intel Pentium or compatible minimum required
	Red Hat Enterprise Linux AS 4.9 with kernel 2.6.9-100 (Update 9)	x64
	Red Hat Enterprise Linux AS 4.0 with kernel 2.6.9-89 (Update 8)	x64
	Red Hat Enterprise Linux AS 4.0 with kernel 2.6.9-89 (Update 8)	Intel Pentium or compatible minimum required
	Red Hat Enterprise Linux AS 4.0 with kernel 2.6.9-78 (Update 7)	Intel Pentium or compatible minimum required
	Red Hat Enterprise Linux AS 4.0 with kernel 2.6.9-78 (Update 7)	x64
	Red Hat Enterprise Linux AS 4.0 with kernel 2.6.9-67 (Update 6)	x64
	Red Hat Enterprise Linux AS 4.0 with kernel 2.6.9-67 (Update 6)	Intel Pentium or compatible minimum required
	Red Hat Enterprise Linux AS 4.0 with kernel 2.6.9-55 (Update 5)	Intel Pentium or compatible minimum required
	Red Hat Enterprise Linux AS 4.0 with kernel 2.6.9-55 (Update 5)	x64
	Red Hat Enterprise Linux AS 4.0 with kernel 2.6.9-42 (Update 4)	x64
	Red Hat Enterprise Linux AS 4.0 with kernel 2.6.9-42 (Update 4)	Intel Pentium or compatible minimum required
	Red Hat Enterprise Linux AS 4.0 with kernel 2.6.9-34 (Update 3)	Intel Pentium or compatible minimum required
	Red Hat Enterprise Linux AS 4.0 with kernel 2.6.9-34 (Update 3)	x64
	Red Hat Enterprise Linux 6 Advanced Platform with kernel 2.6.32-71	Intel Pentium or compatible minimum required

	Red Hat Enterprise Linux 6 Advanced Platform with kernel 2.6.32-71	x64
	Red Hat Enterprise Linux 6 Advanced Platform with kernel 2.6.32-131 (Update 1)	x64
	Red Hat Enterprise Linux 5 Advanced Platform with kernel 2.6.18-92 (Update 2)	Intel Pentium or compatible minimum required
	Red Hat Enterprise Linux 5 Advanced Platform with kernel 2.6.18-92 (Update 2)	x64
	Red Hat Enterprise Linux 5 Advanced Platform with kernel 2.6.18-8	Intel Pentium or compatible minimum required
	Red Hat Enterprise Linux 5 Advanced Platform with kernel 2.6.18-8	x64
	Red Hat Enterprise Linux 5 Advanced Platform with kernel 2.6.18-53 (Update 1)	x64
	Red Hat Enterprise Linux 5 Advanced Platform with kernel 2.6.18-53 (Update 1)	Intel Pentium or compatible minimum required
	Red Hat Enterprise Linux 5 Advanced Platform with kernel 2.6.18-238 (Update 6)	Intel Pentium or compatible minimum required
	Red Hat Enterprise Linux 5 Advanced Platform with kernel 2.6.18-238 (Update 6)	x64
	Red Hat Enterprise Linux 5 Advanced Platform with kernel 2.6.18-194 (Update 5)	Intel Pentium or compatible minimum required
	Red Hat Enterprise Linux 5 Advanced Platform with kernel 2.6.18-194 (Update 5)	x64
	Red Hat Enterprise Linux 5 Advanced Platform with kernel 2.6.18-164 (Update 4)	Intel Pentium or compatible minimum required
	Red Hat Enterprise Linux 5 Advanced Platform with kernel 2.6.18-164 (Update 4)	x64
	Red Hat Enterprise Linux 5 Advanced Platform with kernel 2.6.18-128 (Update 3)	x64
	Red Hat Enterprise Linux 5 Advanced Platform with kernel 2.6.18-128 (Update 3)	Intel Pentium or compatible minimum required
	SUSE LINUX (SLES)	
	SuSE Linux 11 Enterprise Server with kernel 2.6.32.12-0.7 (Update 1)	Intel Pentium or compatible processors
	SuSE Linux 11 Enterprise Server with kernel 2.6.32.12-0.7 (Update 1)	x64
	SuSE Linux 11 Enterprise Server with kernel 2.6.27.19-5	x64
	SuSE Linux 11 Enterprise Server with kernel 2.6.27.19-5	Intel Pentium or compatible processors
	SuSE Linux 10 Enterprise Server with kernel 2.6.16.60-0.54.5 (Update 3)	Intel Pentium or compatible processors
	SuSE Linux 10 Enterprise Server with kernel 2.6.16.60-0.54 (Update 3)	Intel Pentium or compatible processors
	SuSE Linux 10 Enterprise Server with kernel 2.6.16.60-0.34 (Update 2)	Intel Pentium or compatible processors
	SuSE Linux 10 Enterprise Server with kernel 2.6.16.60-0.21 (Update 2)	Intel Pentium or compatible processors
	SuSE Linux 10 Enterprise Server with kernel 2.6.16.60-0.21 (Update 2)	x64
	SuSE Linux 10 Enterprise Server with kernel 2.6.16.46-0.12 (Update 1)	Intel Pentium or compatible processors
SOLARIS	Solaris 9 64-bit with Service Packs 111711-02 and 111712-02	Ultra2 or higher recommended
	Solaris 9 4/04 64-bit	Ultra2 or higher recommended
	Solaris 10.x with a minimum of SunOS (Sparc) Patch 119963-14	Ultra2 or higher recommended
	Solaris 10.x (6/06 and higher) 64 bit	Ultra2 or higher recommended

CLUSTER - SUPPORT

The software can be installed on a Cluster if clustering is supported by the above-mentioned operating systems.

For information on supported cluster types, see Clustering - Support.

HARD DRIVE

250 MB minimum of hard disk space for software

50 MB of additional hard disk space for log file growth

719 MB of temp space required for install (where the temp folder resides)

3.5 KB per file of cache partition

MEMORY

256 MB RAM or higher recommended total system memory

SOLARIS ZONES/CONTAINERS SUPPORT

The File Archiver Agent should be installed on the global zone, and cannot be installed on a non-global zone.

The global instance of the File Archiver Agent can be used to archive data on a non-global zone.

For a comprehensive list of supported components, see Unix Virtualization.

AIX LPAR/WPAR SUPPORT

Data protection on Logical Partitioning (LPAR) and Workload Partitioning (WPAR) is supported.

PERIPHERALS

DVD-ROM drive

Network Interface Card

MISCELLANEOUS

NETWORK

TCP/IP Services configured on the computer.
On Solaris computers, the operating system must have been installed with at least the `user level software` option selected.

LUSTRE FILE SYSTEM

Lustre File System version 2.0.0.1 is supported on Red Hat Enterprise Linux 5.x computers with kernel 2.6.18-164.

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
	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`

name for policy module and the file.	`(system_u:object_r:texrel_shlib_t,s0)`
For example: When you are creating a policy module for backup_IDA application, you can use the following file name: `backup_IDA.fc`	`/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.

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

Getting Started - File Archiver Deployment

WHERE TO INSTALL

The Unix File Archiver Agent is used to archive Unix machine data.

Install the software directly on the computer hosting the global zone or the Unix Server that you wish to protect. Make sure the computer satisfies the minimum requirements specified in the System Requirements.

The global instance of the File Archiver Agent can be used to archive and restore/recall data on a non-global zone.

Follow the steps given below to install the Unix File Archiver Agent.

INSTALLATION

The software can be installed using one of the following methods:

METHOD 1: INTERACTIVE INSTALL

Use this procedure to install the software directly on client computer.

METHOD 2: INSTALL SOFTWARE FROM COMMCELL CONSOLE

Use this procedure to remotely install the software on a client computer.

BEFORE YOU BEGIN

Download Software Packages
Download the latest software package to perform the install.

System Requirements
Verify that the computer in which you wish to install the software satisfies the System Requirements.

METHOD 1: INTERACTIVE INSTALL

1.   Run the following command from the Software Installation Disc:

   ./cvpkgadd

2.   The product banner and other information is displayed.

   Press **Enter**.

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

4.   Press **Enter**.

```
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.   Press **Enter**.

```
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]
```

6.   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 interface name that you wish to use as default, and then press **Enter**.

   The interface names 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]

7.   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.

Physical Machine Client name: [angel]

8.   Type the appropriate number to install **File Archiver for UNIX Agent**.

Install Calypso on physical machine angel

A confirmation screen will mark your choice with an "**X**".

Please select the Calypso module(s) that you would like to install.

Type **d** for **Done**, and press **Enter**.

[ ] 1) MediaAgent [1301] [CVGxMA]

[ ] 2) UNIX File System iDataAgent [1101] [CVGxIDA]

[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

9.   Press **Enter**.

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

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

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

- Select **Download from the software provider website** to download the latest software scripts. Make sure you have internet access.
- Select **Use the one in the installation media** to install the software scripts from the package or share from which the installation is currently being 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.

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

11.   Press **Enter**.

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]

12.

Please specify where you want us to install Calypso binaries.

Press **Enter** to accept the default path.

It must be a local directory and there should be at least 176MB 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".

- If you want to specify a different path, type the path and then press **Enter**.
- If you want to install the software binaries to an NFS shared drive, specify the directory on which you have mounted the NFS file system and then press **Enter**.

Installation Directory: [/opt]

In order to make sure that the client computer has `read/write` access to NFS shared drive, review the steps described in Installing Software Binaries to an NFS Shared Drive.

Do not use the following characters when specifying the path:

!@#$%^&*():/?\

13.   Press **Enter** to accept the default location.

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".

- Enter a path to modify the default location and press **Enter**.
- All the modules installed on the computer will store the log files in this directory.

Log Directory: [/var/log]

14.   Type **no**.

Most of Software 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.

If entering **Yes**, go to Step 16.

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 Software processes, you will need to specify the access permissions later.

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

<table>
<tr><td>

15. Type **d** for done.

</td><td>

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

Access Permissions for Other Users

Installer will assign full access rights to root user and
its belonging group
for all installed Software files and its processes.

For any other users, you can specify the access
permissions now.

However, since you chose not to assign a dedicated group
in previous step,
make sure you specify sufficient access rights for other
users if you are also
planning to install Software agents involving third party
software protection.

[X] 1) Allow read permission to other users
[X] 2) Allow write permission to other users
[X] 3) Allow execute permission to other users

[a=all n=none r=reverse q=quit d=done >=next <=previous ?
=help]
Enter number(s)/one of "a,n,r,q,d,>,<,?" here:
```

</td></tr>
<tr><td>

16. If you indicated **Yes** in Step 14., you will be prompted for the group name that must be used to launch processes.

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

- See your Unix systems administrator for assistance in creating a user group.

</td><td>

```
Please enter the name of the group which will be assigned
to all Software files and on behalf of which all Software

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: sky1

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
"sky1".

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

</td></tr>
<tr><td>

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**.

</td><td>

```
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 : [8400]

Port Number for EvMgrC: [8402]
```

</td></tr>
<tr><td>

18. If you do not wish to configure the firewall services, press **Enter**.

If this computer is separated from the CommServe by firewall(s), type **Yes** and then press **Enter**.

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

</td><td>

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

</td></tr>
<tr><td>

19. Type the fully qualified CommServe host name and press **Enter**.

Ensure that the CommServe is accessible before typing the name; otherwise the installation will fail.

</td><td>

```
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: mycommserve.company.com
```

</td></tr>
<tr><td>

20. Press **Enter**.

</td><td>

```
Commcell Level Global Filters are set through Calypso
GUI's Control Panel in order to filter out certain
directories or files from backup Commcell-widely. If you
turn on the Global filters, they will be effective to the
default subclient. There are three options you can choose
to set the filters.

1) Use Cell level policy

2) Always use Global filters

3) Do not use Global filters

Please select how to set the Global Filters for the
default subclient? [1]
```

</td></tr>
<tr><td>

21. Type the appropriate number to select the **Client Group** and press **Enter**.

This screen will be displayed only if Client Groups are configured for the CommCell

</td><td>

```
Client Group(s) is currently configured on CommServe
mycommserve.company.com. Please choose the group(s) that
you want to add this client angel.company.com to. The
selected group(s) will be marked (X) and can be deselected
if you enter the same number again. After you are finished
with the selection, select "Done with the Selection".

[ ] 1) Unix
```

</td></tr>
</table>

```
[ ] 2) DR

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

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

22. Enter the number corresponding to the storage policy through which you want to back up the External Data Connector and press **Enter**.

```
Please select one storage policy for this IDA from the
list below:

1) SP_StandAloneLibrary2_2

2) SP_Library3_3

3) SP_MagLibrary4_4

Storage Policy: [1]
```

If you do not have Storage Policy created, this message will be displayed.

You may not be prompted for user input.

You can create the Storage Policy later in step 24.

```
There seem to be no Storage Policies configured on the
CommServe. Before you can run any backups of this IDA, you
will need to install a MediaAgent, create a Storage Policy
and assign it to all subclients..

Adjusting modes and permissions of files

Successfully installed Calypso
```

23. Type **3** to the **Exit** option and press **Enter**.

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
angel.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 angel.company.com

2) Install Calypso on a virtual machine

3) Exit

Your choice: [3]
```

If you already have a storage policy selected in step 22, click the Next button available on the bottom of the page to proceed to the Configuration section.

If you do not have Storage Policy created, follow the procedure given below.

24.
1. From the CommCell Browser, navigate to **Policies**.

2. Right-click the **Storage Policies** and then click **New Storage Policy**.

3. Follow the prompts displayed in the Storage Policy Wizard. The required options are mentioned below:
   ○ Select the Storage Policy type as **Data Protection and Archiving** and click **Next**.
   ○ Enter the name in the **Storage Policy Name** box and click **Next**.
   ○ From the **Library** list, click the name of a disk library to which the primary copy should be associated and then click **Next**.

   Ensure that you select a library attached to a MediaAgent operating in the current release.

   ○ From the **MediaAgent** list, click the name of a MediaAgent that will be used to create the primary copy and then click **Next**.
   ○ For the device streams and the retention criteria information, click **Next** to accept default values.
   ○ Select **Yes** to enable deduplication for the primary copy.
   ○ From the **MediaAgent** list, click the name of the MediaAgent that will be used 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 and then click **Next**.

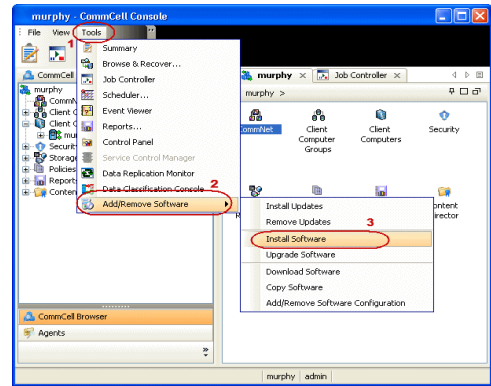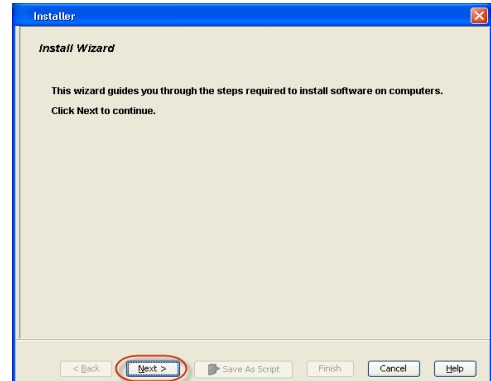   ○ Review the details and click **Finish** to create the Storage Policy.

METHOD 2: INSTALL SOFTWARE FROM COMMCELL CONSOLE

1. From the CommCell Browser, select **Tools** | **Add/Remove Software** | **Install Software.**
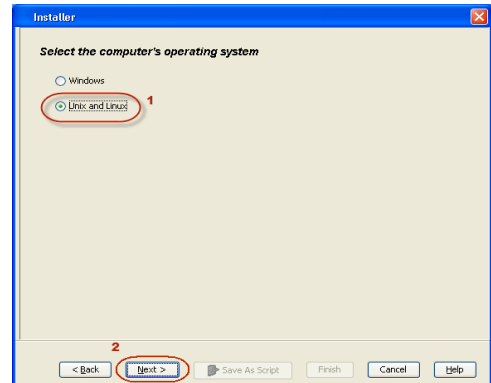
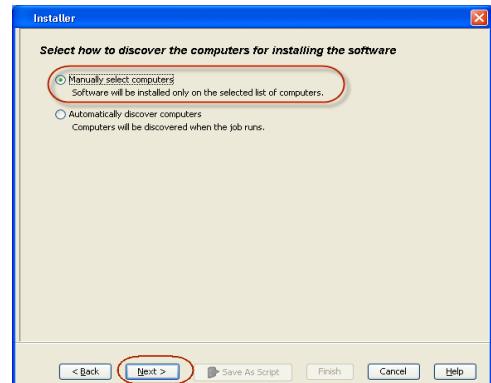2.   Click **Next**.

3.   Select **Unix and Linux**.

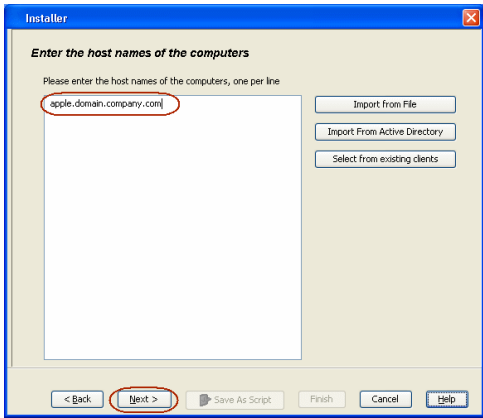   Click **Next**.

4.   Select **Manually Select Computers**.

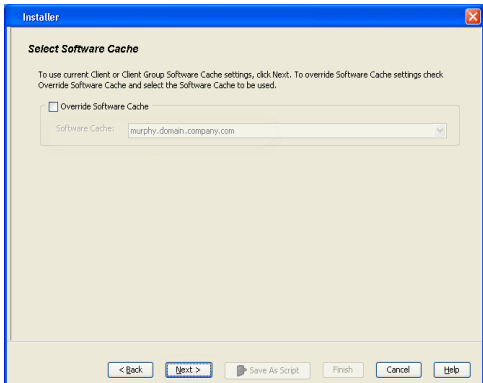   Click **Next**.

5.   Enter the fully qualified domain name of the computer in which you wish to install.

      For example: `apple.domain.company.com`

      The **File Archiver for UNIX Agent** will be installed on this client computer.
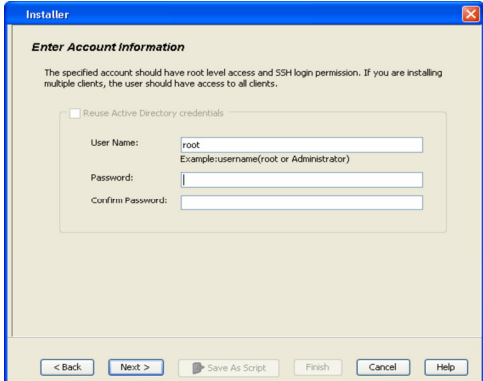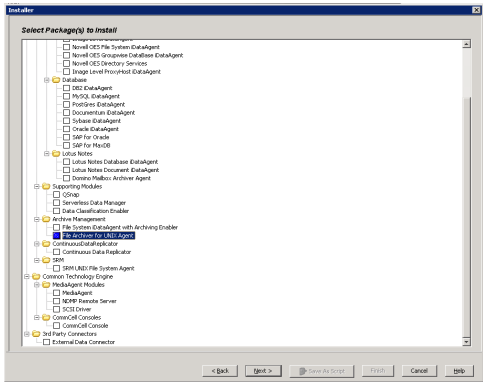
      Click **Next**.

6. Click **Next**.

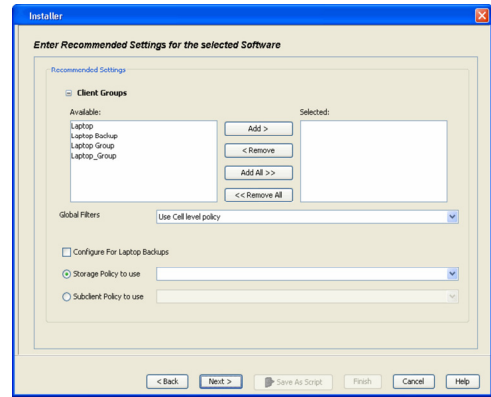**7.** Specify **UserName** and **Password** of client computer.

Click **Next**.

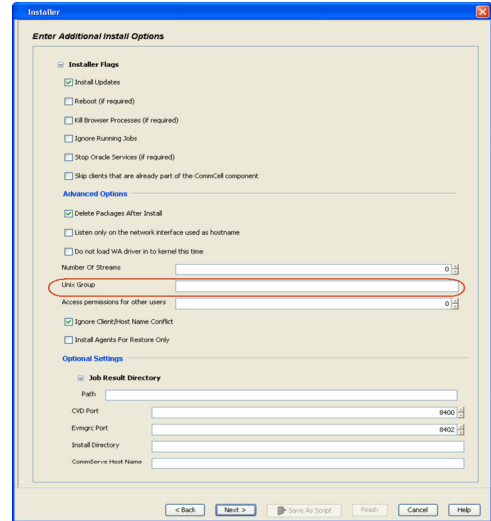**8.** Select **File Archiver for UNIX Agent**.

Click **Next**.

9. ● Select **Client Group** from **Available** and click **Add**.

Do not add more than one Client Group.

● Select a **Storage Policy** from the drop-down list. Click **Next**.
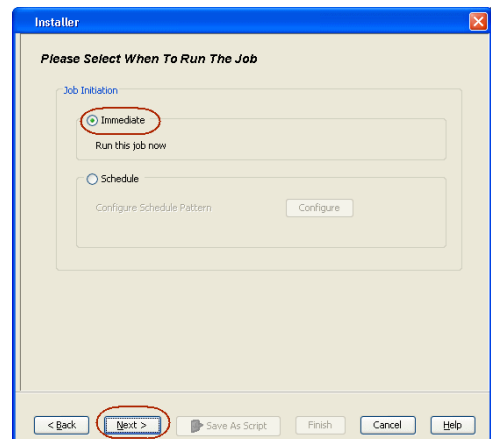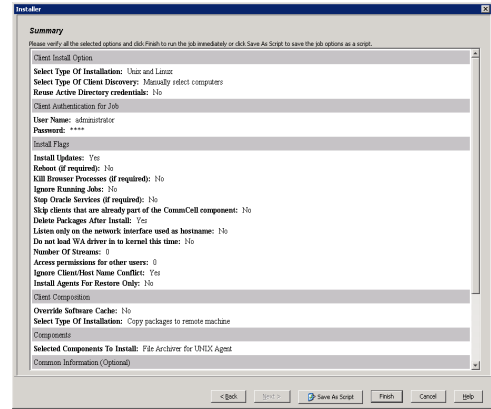
10. Click **Next**.

11. Select **Immediate**.
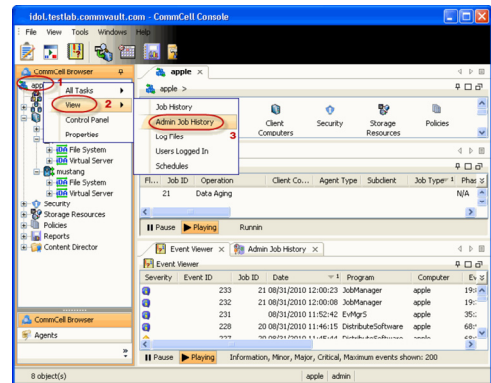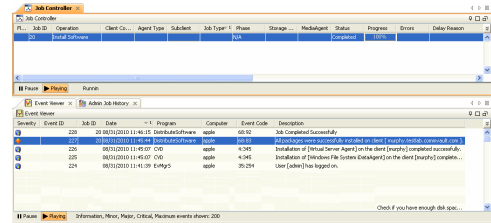
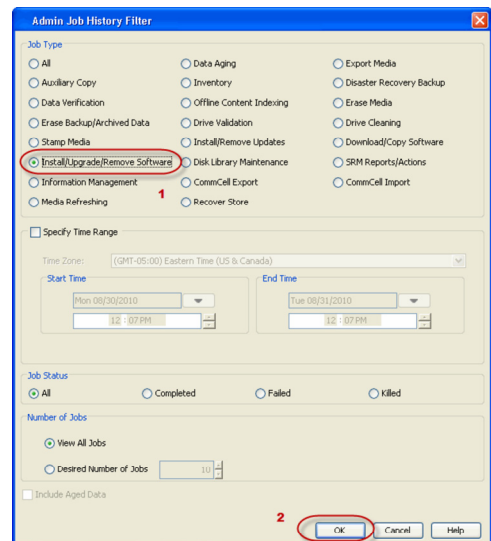Click **Next**.

12. Click **Finish**.

13. You can track the progress of the job from the **Job Controller** or **Event Viewer** window.

14. Once the job is complete, right-click the **CommServe** computer, click **View** and then click **Admin Job History**.
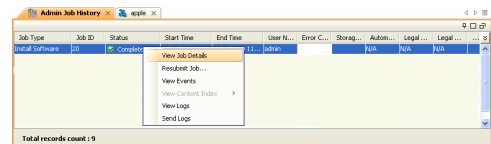

15. Select **Install/Upgrade/Remove Software**.

Click **OK**.

16. You can view the following details about the job by right-clicking the job:
- Items that succeeded during the job
- Items that failed during the job
- Details of the job
- Events of the job
- Log files of the job

Getting Started - File Archiver Deployment on a Cluster
SKIP THIS PAGE IF YOU ARE NOT INSTALLING THIS AGENT ON A CLUSTER

Click **Next** ➤ to continue with the configuration.

◀ Previous   Next ▶

WHERE TO INSTALL

The File Archiver Agent for Unix has to be installed on all the nodes of a cluster group. Install the software from the active node. The software is automatically installed on all the available nodes of the cluster.

Make sure the cluster group satisfies the minimum requirements specified in the System Requirements.

In case the software does not gets installed on any node, it is recommended to manually install the software on that particular node.

Follow the steps given below to install the File Archivers for Unix Agent in a Clustered Environment.

1.   Logon to the client computer as root.

2.   If your are installing the software from CD, run the following command to mount the CD:

   `mount -t iso9660,udf /dev/cdrom /mnt/cdrom`

   Run the following command from the Software Installation Package or mount point:

   `./cvpkgadd`

3.   The product banner and other information is displayed.

   Press **Enter**.

4.   Read the license agreement. Type **y** and press **Enter**.

5.   Press **Enter**.

6.   Press **Enter**.

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 interface name that you wish to use as default, and then press **Enter**.

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

8.   Press **Enter**.

BEFORE YOU BEGIN

Download Software Packages
    Download the latest software package to perform the install.

System Requirements
    Verify that the computer in which you wish to install the software satisfies the System Requirements.

```
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]
```

```
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]
```

```
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]
```

```
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]
9.	Type the number associated with the **File Archiver for Unix Agent** and press Enter.	Install Calypso on physical machine angel
		Please select the Calypso module(s) that you would like to install.
		[ ] 1) MediaAgent [1301] [CVGxMA]
		[ ] 2) UNIX File System iDataAgent [1101] [CVGxIDA]
		[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
10.	A confirmation screen will mark your choice with an "**X**".	Install Calypso on physical machine angel
	Type **d** for **Done**, and press **Enter**.	Please select the Calypso module(s) that you would like to install.
		[ ] 1) MediaAgent [1301] [CVGxMA]
		[ ] 2) UNIX File System iDataAgent [1101] [CVGxIDA]
		[a=all n=none r=reverse q=quit d=done >=next <=previous ? =help]
		Enter number(s)/one of "a,n,r,q,d,>,<,?" here:d
11.	Press **Enter**.	Do you want to use the agents for restore only without consuming licenses? [no]
12.	Type the appropriate number to install the latest software scripts and press **Enter**.	Installation Scripts Pack provides extra functions and latest support and fix performed during setup time. Please specify how you want to get this pack.
	● Select **Download from the software provider website** to download the latest software scripts. Make sure you have internet access.	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.
	● Select **Use the one in the installation media** to install the software scripts from the package or share from which the installation is currently being performed.	1) Download from the software provider website.
	● 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.	2) Use the one in the installation media
		3) Use the copy I already have by entering its unix path
		Your choice: [1] 2
13.	Press **Enter**.	Keep Your Install Up to Date - Latest Service Pack
	It is recommended to download the latest Service pack(s). Type **Yes** and press **Enter** to automatically install the available updates during installation.	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]
14.	Press **Enter** to accept the default path.	Please specify where you want us to install Calypso binaries.
	● If you want to specify a different path, type the path and then press **Enter**.	It must be a local directory and there should be at least 176MB 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".
	● If you want to install the software binaries to an NFS shared drive, specify the directory on which you have mounted the NFS file system and then press **Enter**.	
	In order to make sure that the client computer has read/write access to NFS shared drive, review the steps described in Installing Software Binaries to an NFS Shared Drive.	Installation Directory: [/opt]
	Do not use the following characters when specifying the path:	
	!@#$%^&*():/?\	
15.	Press **Enter** to accept the default location.	Please specify where you want to keep Calypso log files.
	● Enter a path to modify the default location and press **Enter**.	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".
	● All the modules installed on the computer will store the log files in this directory.	
		Log Directory: [/var/log]
16.	Press **Enter**.	Most of Software 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 Software processes, you will need to specify the access permissions later.

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

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

17. Type the **Group name** and press **Enter**.

Press **Enter** again.

Please enter the name of the group which will be assigned to all Software files and on behalf of which all Software 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: sky1

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 "sky1".

Press <ENTER> to continue ...

18. Press **Enter** to accept the default value for **Number of Streams**.

You can type the **Number of Streams** that you plan to run at the same time and then press **Enter**.

Number of Streams

IMPORTANT : Please read install document "Configure Kernel Parameters - Unix/Macintosh" from "Books Online" before you start configuring kernel parameters. 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]

19. Press **Enter** if you do not want to apply the changes now.

- If you want to apply the changes now, type **Yes** and then press **Enter**.
- You will come across this prompt when you install the software on the earlier versions of Solaris.

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]

21. Press **Enter**.

You will see this prompt if you have accepted the default **no** and pressed **Enter** in the above step.

Changes saved into /etc/system.gal.1744

Press <ENTER> to continue.

22. Press **Enter**.

You will see this message if you have accepted the default answer and pressed **Enter** in step 19.

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
```
Press <ENTER> to continue.

23. 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**.

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 : [8400]

Port Number for EvMgrC: [8402]

24. If you do not wish to configure the firewall services, press **Enter**.

If this computer is separated from the CommServe by firewall(s), type **Yes** and then press **Enter**.

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

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

25. Type the fully qualified CommServe host name and press **Enter**.

Ensure that the CommServe is accessible before typing the name; otherwise the installation will fail.

```
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: mycommserve.company.com
```

26. Type the appropriate number to select the **Client Group** and press **Enter**.

This screen will be displayed only if Client Groups are configured for the CommCell

```
Client Group(s) is currently configured on CommServe
mycommserve.company.com. Please choose the group(s) that
you want to add this client angel.company.com to. The
selected group(s) will be marked (X) and can be deselected
if you enter the same number again. After you are finished
with the selection, select "Done with the Selection".

[ ] 1) Unix

[ ] 2) DR

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

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

27. A confirmation screen will mark your choice with an "**X**".

Type **d** for **Done**, and press **Enter**.

```
Client Group(s) is currently configured on CommServe
cs.company.com. Please choose the group(s) that you want
to add this client client.company.com to. The selected
group(s) will be marked (X) and can be deselected if you
enter the same number again. After you are finished with
the selection, select "Done with the Selection".

[ ] 1) Unix

[X ] 2) DR

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

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

28. Enter the number associated with the storage policy you want use and press **Enter**.

```
Please select one storage policy for this IDA from the
list below:

1) SP_StandAloneLibrary2_2

2) SP_Library3_3

3) SP_MagLibrary4_4

Storage Policy: [1]
```

If you do not have Storage Policy created, this message will be displayed. You may not be prompted for user input.

You can create the Storage Policy later in step 39.

```
There seem to be no Storage Policies configured on the
CommServe. Before you can run any backups of this IDA, you
will need to install a MediaAgent, create a Storage Policy
and assign it to all subclients..

Adjusting modes and permissions of files

Successfully installed Calypso
```

29. Type **2** to install **File Archiver for Unix** on a Virtual machine , and press **Enter**.

```
Cluster Support

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
angel.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 angel.company.com

2) Install Calypso on a virtual machine

3) Exit

Your choice: [2]
```

30. 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 interface name that you wish to use as default, and then press **Enter**.

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

```
Virtual Machine Host Name

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.

The name to be entered will be used by certain Calypso
```

CommServe to talk to this

virtual machine. Datapipe Interface Pairs used for the backup data traffic can be customized later in the Calypso Java GUI.

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

Virtual Machine Host Name: docm.company.com

31.	Type the **Virtual Machine Client Name**, and press **Enter**.	Virtual Machine Client Name

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: [docm]

32.	Type the number associated with the **Unix File System** *i***DataAgent** and press **Enter**.	Install Calypso on virtual machine docm

Please select the Calypso module(s) that you would like to install.

[ ] 1) MediaAgent [1301] [CVGxMA]

[ ] 2) UNIX File System iDataAgent [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

33.	A confirmation screen will mark your choice with an "**X**".	Install Calypso on virtual machine docm
	Type **d** for **Done**, and press **Enter**.	

Please select the Calypso module(s) that you would like to install.

[ ] 1) MediaAgent [1301] [CVGxMA]

[x] 2) UNIX File System iDataAgent [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:d

34.	Press **Enter**.	Do you want to use the agents for restore only without consuming licenses? [no]
35.	Specify the path for the **Job Results directory**, and press **Enter**	Calypso Job Results Directory Please specify the name for the JobResults directory.Since you are installing Calypso on a virtual machine, the JobResults directory must reside on a shared disk and should have at least 20MB of free space available. The directory will be used to store intermediate data that should be passed from one backup phase to another.
	If Job Results directory does not exist, it prompts you to create it. Type **Yes** to create it.	

JobResults Directory:

36.	Enter the number associated with the storage policy you want use and press **Enter**.	Please select one storage policy for this IDA from the list below:

1) SP_StandAloneLibrary2_2

2) SP_Library3_3

3) SP_MagLibrary4_4

Storage Policy: [1]

	If you do not have Storage Policy created, this message will be displayed. You may not be prompted for user input.	There seem to be no Storage Policies configured on the CommServe. Before you can run any backups of this IDA, you will need to install a MediaAgent, create a Storage Policy and assign it to all subclients..
	You can create the Storage Policy as shown in step 39.	

Adjusting modes and permissions of files

Successfully installed Calypso

37.	Type **4** to the **Exit** option and press **Enter**.	Calypso is currently configured on the following virtual/physical machines.
	The installation is now complete.	

Now you have an option of either installing certain Calypso on another virtual machine

or adding a new package to the existing installations.1) Add a new package to PM angle(angel.mycompany.com)

2) Add a new package to VM docm (docm.mycompany.com)

3) Install Calypsopackages on a new virtual machine

4) Exit this menu

Your choice: [1] 4

38.	Type **3** to the **Exit** option, and press **Enter**.	Install a new Instance?

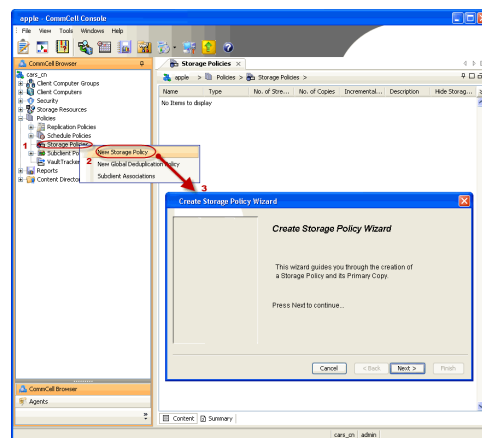Calypso now supports the concept of instances, each of

which can be installed to a separate CommServe and be totally independent of others. Instances are not the same as the virtual machines on a cluster, in fact, you will be given a choice to configure one or more virtual machines later. Contrary to previous releases of Calypso (6.1 and older), all virtual machines installed on the same host now share the same set of binaries and the same set of services.

Instances, on the other hand, have unique set of binaries and services and one situation where it is useful is when you want to back up the same host to several CommServes.

You already have one instance configured.

1) Add agents to existing Instance001 going to CS mycommserve.company.com

2) Create a new instance of Calypso

3) Exit this menu

Your choice: 3

If you already selected a storage policy in step 28, proceed to the Configuration section.

If you do not have Storage Policy created, follow the procedure given below.

39.

1. From the CommCell Browser, navigate to **Policies**.

2. Right-click the **Storage Policies** and then click **New Storage Policy**.

3. Follow the prompts displayed in the Storage Policy Wizard. The required options are mentioned below:
   - Select the Storage Policy type as **Data Protection and Archiving** and click **Next**.
   - Enter the name in the **Storage Policy Name** box and click **Next**.
   - From the **Library** list, click the name of a disk library to which the primary copy should be associated and then click **Next**.

     Ensure that you select a library attached to a MediaAgent operating in the current release.
   - From the **MediaAgent** list, click the name of a MediaAgent that will be used to create the primary copy and then click **Next**.
   - For the device streams and the retention criteria information, click **Next** to accept default values.
   - Select **Yes** to enable deduplication for the primary copy.
   - From the **MediaAgent** list, click the name of the MediaAgent that will be used 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 and then click **Next**.
   - Review the details and click **Finish** to create the Storage Policy.

40. After install, `cvclusternotify.sh` 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.

- During node shutdown, the script notifies the driver to stop monitoring the shared volume on this node.
- During node startup, the script notifies the driver to start monitoring the shared volume on this node.

Usage:

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

Where:

`cvclusternotify` - Program to notify Calypso of cluster failovers.

This command notifies the drivers to stop or start monitoring the file system.

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`

  This will notify the driver to stop monitoring the shared file systems on the current node.

- To Start Up:

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

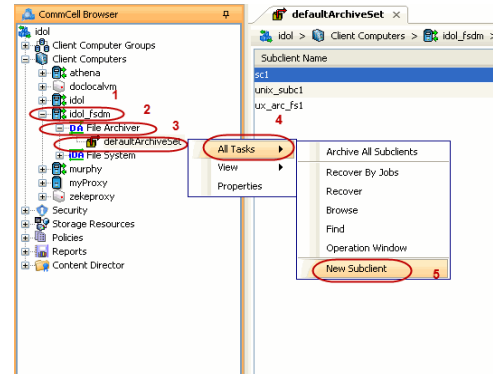 This will notify the driver to start monitoring the shared file systems on the current node.

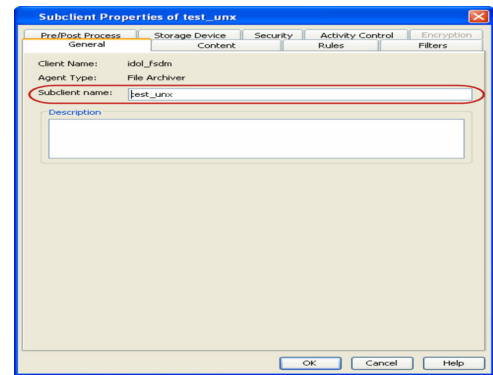# Getting Started - File Archiver Configuration

CONFIGURATION

Once the Unix File Archiver Agent has been installed, configure a Subclient to facilitate archiving. The following sections provide the necessary steps required to create and configure a subclient for running the first archive job.
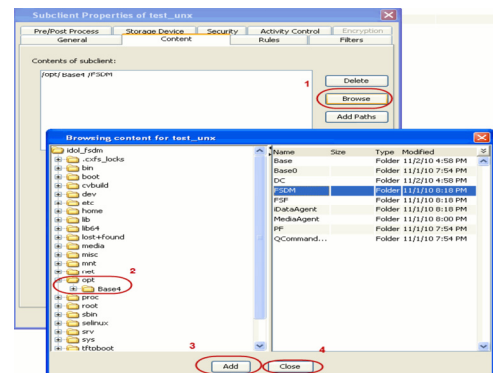
1.
- From the CommCell Browser, navigate to **<Client> | File Archiver | Default Archive Set**.
- Right-click **Default Archive Set | All Tasks**
- Click **New Subclient**.

2.   Enter **Subclient Name**.

3.
- Click the **Content** tab.
- **Browse** to the folder that has files to be archived.
- Select the folder and click **Add.**
- Click **Close**.

4.
- Click the **Storage Device** tab.
- Select the **Storage Policy** from the drop down list.
- Click **OK**.

  If you do not have a Storage Policy created, follow the steps given below to create a Storage Policy.

5.

1. Click **Create Storage Policy**.

2. Follow the prompts displayed in the Storage Policy Wizard. The required options are mentioned below:

   ○ Select the Storage Policy type as `Data Protection and Archiving`.

   ○ Select `No` to allow legal hold to use the policy.

   ○ Specify the name of the Storage Policy.

   ○ Specify the name of the primary copy. The primary copy is automatically created along with the Storage Policy.

   ○ Select `No` for use of an existing global deduplication policy.

   ○ Specify name of the default library to which the Primary Copy should be associated. This must be a disk library. Ensure that you select a library attached to a MediaAgent operating in the current release.

   ○ Select the MediaAgent.

   ○ Verify the device streams and the retention criteria information.

   ○ Select `Yes` to enable deduplication for the primary copy. Select the Enable Client Side Deduplication option.

   ○ Name of the Deduplication Store, MediaAgent hosting the Deduplication Store, and the location of the Deduplication Store.

   ○ Review the details and click **Finish** to create the Storage Policy. The primary copy is also created.

Getting Started - File Archiver Archive

PERFORM AN ARCHIVE

After configuring a subclient and a storage policy, you are ready to perform your first archive.

WHAT GETS ARCHIVED

The Unix File Archiver archives the following:

OPERATING SYSTEM	ARCHIVED FILE SYSTEMS
AIX	Journal File System 2 (JFS2)
	IBM General Parallel File System (GPFS)
	VERITAS File System (VxFS)
	VERITAS Cluster File System (VxCFS)
HP-UX	VERITAS File System (VxFS)
Linux	'X' File System (XFS)
	B-tree File System (Btrfs)
	Extended 3 File System (ext3)
	Extended 4 File System (ext4)
	IBM General Parallel File System (GPFS)
	X9000 IBRIX File System (IBRIXFS) 6.x
	PolyServe Matrix Server
	VERITAS File System (VxFS)
	VERITAS Cluster File System (VxCFS)
	Lustre File System (Clustered File System)
Red Hat Linux 6.x	GFS2 (Clustered File System)
	The default Extended 2 File System (ext2) gets archived when it is compiled as a module.
Novell OES2 Linux	NSS file system
Solaris	Unix File System (UFS)
	VERITAS File System (VxFS)
	Zettabyte File System (ZFS on Solaris 10 6/06)

WHAT DOES NOT GET ARCHIVED

The following file types/objects are automatically filtered out of archive operations by the system, and will not be archived.

- Sparse files (Example: File Archiver stub files)
- Install directory
- Job Results directory
- Log files directory
- `/usr` system directory
- `/kernel` system directory
- `/etc` system directory
- `/tmp` directory
- Extended attributes in the OES Linux data
- Stubs originating from the OES Linux Operating System in a Netware Operating System

The following section provides step-by-step instructions for performing your first archive:

1.
   - From the CommCell Console, navigate to **Client Computer** | **File Archiver** | **defaultArchiveSet**.
   - Right-click the **Subclient** and click **Archive**.

2.
- Select **Immediate** to run the job immediately.
- Click **OK**.
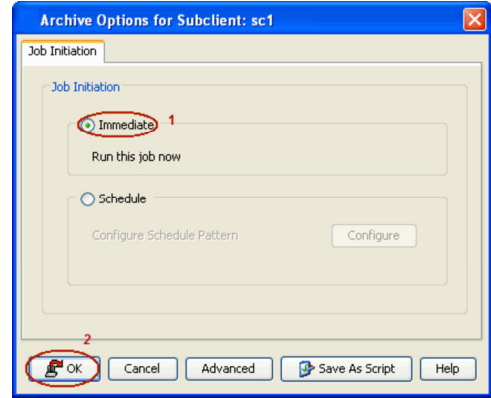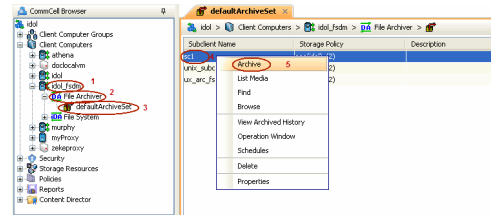
3. You can track the progress of the job from the **Job Controller** or **Event Viewer** window of the CommCell console.
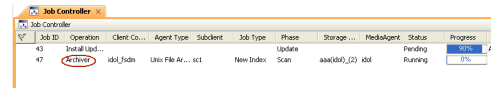
4. Once the archiving process is completed, files that meet the stubbing rules are stubbed.
- **Stubs** are placeholders of the original data after it has been migrated to the secondary storage.
- Stubs replace the archived files in the location selected by the user during the archive.
- After stubbing, the size of the files on the disk reduces to a single block.

Files before stubbing

Files after stubbing

5. Once job is complete, view the details of job from the **Archived History**.
- Right-click the subclient and select **View Archived History**.
- Click **OK**.
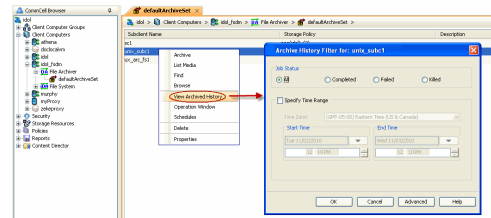
6. You can view the following details about the job by right-clicking the job:

- Details of the job
- Events of the job
- Log files of the job
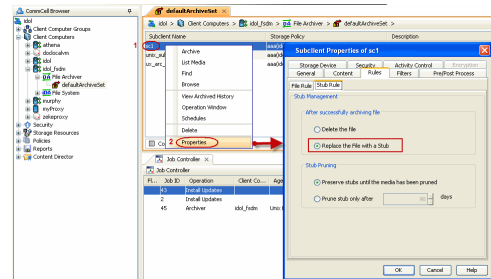- Media associated with the job
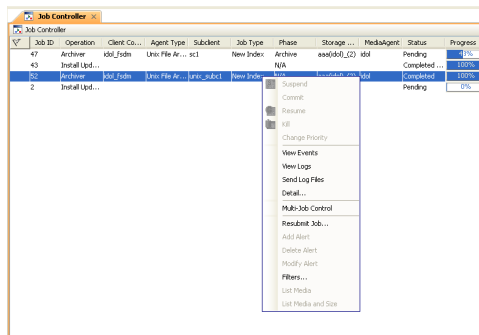
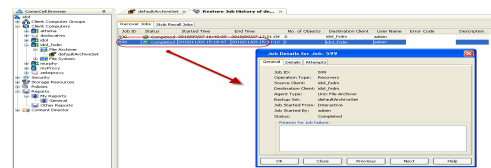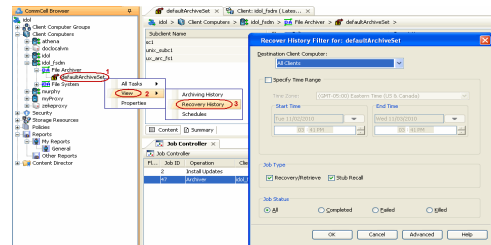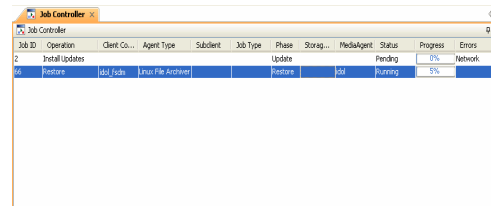# Getting Started - File Archiver Recover
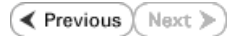
PERFORM A DATA RECOVERY

It is recommended that you perform a recovery operation of an archived file after your first archive operation to understand the process. Follow the steps given below to perform a restore of a file or multiple files from a Unix terminal or console window.

1.
- Open a Terminal or Console Window.
- Perform an action that executes an open and read on an archived file to initiate the recovery operation. For example, you can use the `vi` or `cat` commands to do this:
  - `vi` *<path><filename>*
  - `cat` *<path><filename>*

2.
- You can track the progress of the job from the **Job Controller** or **Event Viewer** window of the CommCell console.
- Multiple stub recoveries are submitted to the Job Controller as one job called a *Persistent Recovery* job.

3.
- Once job is complete, view the details of job from the **Recover History**.
- Right-click the **ArchiveSet** and select **View | Recovery History**.
- Click **OK**.

4.
- Right-click the job and select **View Job Details**.

5.
- If the subclient is configured to create stubs, by choosing the option **Replace the File with a Stub**, files that qualify the archiving rule will get stubbed. You can restore stubs following the same steps listed above (step 1 - step 4).

6.
- After recovery, stubs are replaced by files in the location specified.

Stubbed files:

Recovered files:

Advanced Configuration - File Archiver

TABLE OF CONTENTS

UNDERSTANDING THE COMMCELL CONSOLE

Unix File Archiver agent uses following main components to perform archive and recovery operations from the CommCell Console.

Archive Set - collective information of all the data that needs to be archived for the client.

Subclient - defines the data to be archived.
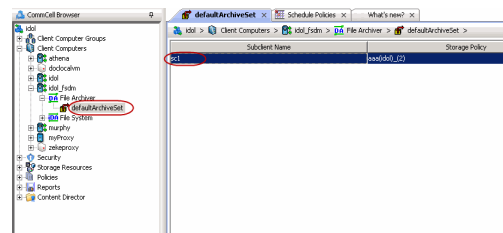
ARCHIVING RULES

In order to perform archiving operations, you need to initially configure archiving rules. Archiving rules specify the criteria for the type of data to be archived. You can configure these rules on a requirement basis.

FILE ACCESS TIME

You can set rules to archive files based on the last accessed date of each file within the volume or folder/directory. Files older than the specified date will be archived.

1. From the CommCell Console, right-click the **Subclient** and click **Properties**.

2. Select **Rules** tab.

3. Select **Enable All Rules**.

4. Enter the number of days elapsed since the file was last accessed **Archive file access time older than _n_ Days**.

5. Select **Any one of the file selection rules are satisfied**.

6. Click **OK**.
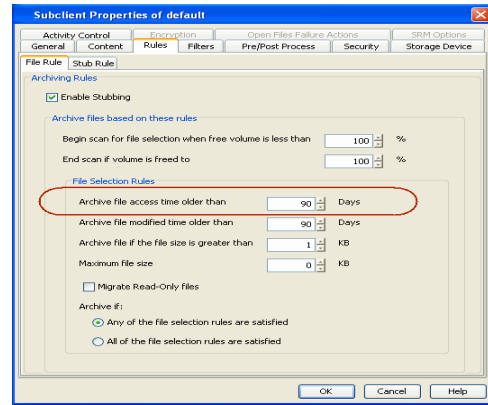
MANAGING FILE ACCESS TIME WHEN UNIX FILE SYSTEM *I*DATAAGENT IS ALSO INSTALLED

Archiving files based on file access times has special considerations. Ordinarily the action of backing up a file using the File System backup agent will cause the file access time to change to the time of the backup. This action may have an undesired effect on the archiver agent if you want to archive files based on access time.

To workaround this situation, you should either use Classic File Scan with the **Preserve File Access Time** option selected as the scan method OR a software snapshot (VSS or Qsnap) to accomplish the backup. If the software snapshot fails (i.e. VSS service unavailable or unable to quiesce the volume), you can use the **Open Files Failure Actions** dialog box to select the desired action to be performed.

FILE MODIFIED TIME

You can also set rules to archive file based on the last modified time. Files that were modified earlier than the specified time will be archived.

1. From the CommCell Console, right-click the **Subclient** and click **Properties**.
2. Select **Rules** tab.
3. Select **Enable All Rules**.
4. Enter the number of days elapsed since the file was last modified **Archive file modified time older than** *n* **Days**.
5. Select **Any one of the file selection rules are satisfied**.
6. Click **OK**.
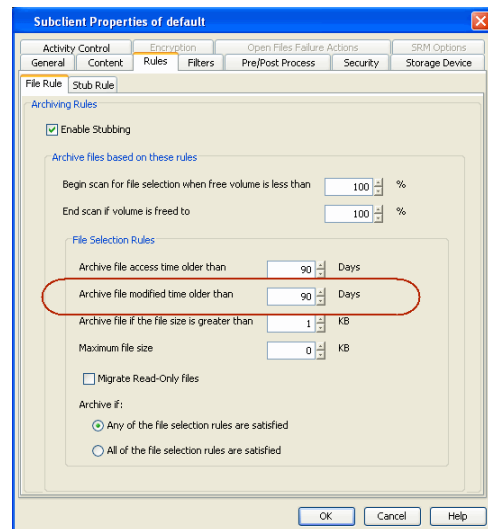
FILE SIZE

You can also set archiving rules to archive files depending on the file size. If a file size within a scanned volume or folder/directory is in between the specified size limit, it will get stubbed.

1. From the CommCell Console, right-click the **Subclient** and click **Properties**.
2. Select **Rules** tab.
3. Select **Enable All Rules**.
4. Enter the minimum file size in **Archive file if size is greater than** *n* **KB**.
5. Enter the maximum file size in **Maximum file size**.

> These options can be used individually or in combination to specify a range.

6. Select **All of the file selection rules are satisfied**.

7. Click **OK**.

For example:

To archive files more than 5KB but less than 20KB:

- Enter 5 KB in **Archive file if size is greater than *n* KB**.
- Enter 20 KB in **Maximum file size**.
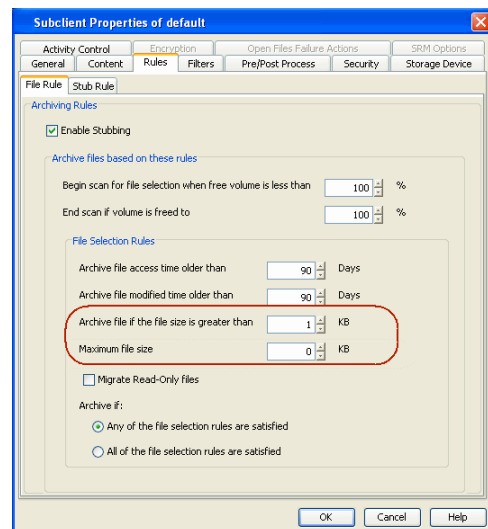
FILE SYSTEM SIZE

The backed up files can be stubbed based on the available free space on the volume. Volumes are periodically checked for available space. If the free space is lesser than the specified low watermark value, the archiving operation begins. The stubbing process stops once it reaches the specified high watermark value.

1. From the CommCell Console, right-click the **Subclient** and click **Properties**.

2. Select **Rules** tab.

3. Select **Enable All Rules**.

4. Enter the low watermark value for the volume in **Begin scan for file selection when free volume is less than n%**.

5. Enter the high watermark value for the volume in **End scan if volume is freed to n%**.

6. Select **All of the file selection rules are satisfied**.

7. Click **OK**.
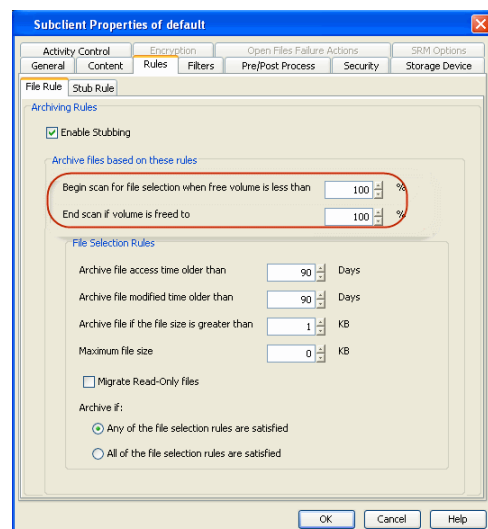
By default files that are less than or equal to the file system block size are skipped from archiving. To archive all the files follow the steps given below:

1. From the CommCell Browser, navigate to **Client Computers**.

2. Right-click the **<*Client*>** and then click **Properties**.

3. Click the **Registry Key Settings** tab.

4. Click **Add**.

5. In the **Name** field, type `sCXHSM_SKIP_FILES_SMALLER_THAN_FSBLOCK`.

6. In the **Location** list, type or select `UnixFsDataMigrator`.

7. In the **Type** list, select **Value**.

8. In the **Value** field, type **N** to archive files that are less than or equal to the file system block size.

9. Click **OK**.
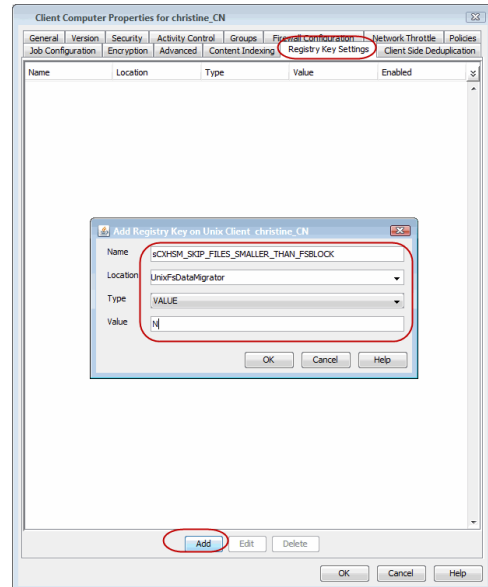
MANAGING ARCHIVED FILES

For an archiving operation, you can set certain stub rules to manage the archived files.

DELETE THE FILE AFTER ARCHIVING

You can choose to delete the file after an archiving operation.

1. From the CommCell Console, right-click the **Subclient** and click **Properties**.
2. Select **Rules** tab.
3. Select **Stub Rule** tab.
4. Select **Delete the File**.
5. Click **OK**.
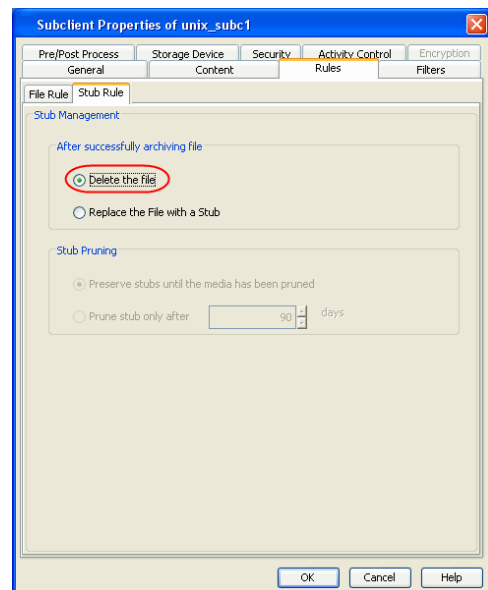
REPLACE FILE WITH A STUB AFTER ARCHIVING

By default, during an archive operation, the file is replaced with a stub. However, if required, you can also set this manually from the **Subclient Properties** window.

1. From the CommCell Console, right-click the **Subclient** and click **Properties**.
2. Select **Rules** tab.
3. Select **Stub Rule** tab.
4. Select **Replace File with a Stub**.
5. Click **OK**.
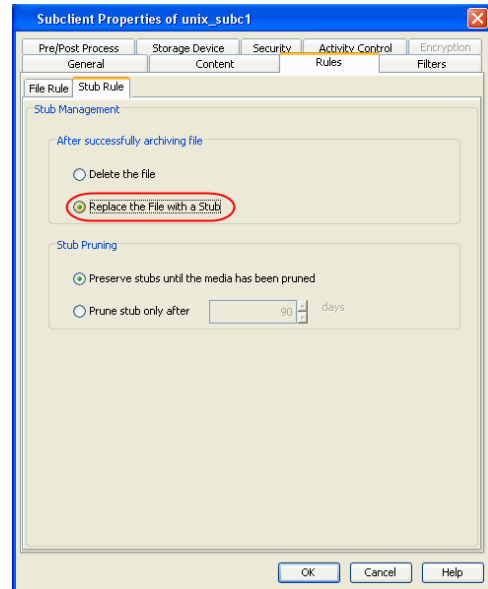
PRUNE THE ARCHIVED FILES (STORAGE RECLAMATION)

By default, the stubs are pruned along with the media. However, you can set the number of days after which the stubs will be pruned.

1. From the CommCell Console, right-click the **Subclient** and click **Properties**.

2. Select **Rules** tab.

3. Select **Stub Rules**.

4. Select **Replace File with a Stub**.

5. Select **Prune Stubs Only After <n> days**.

6. Enter the number of days after which the stubs will be pruned.

7. Click **OK**.
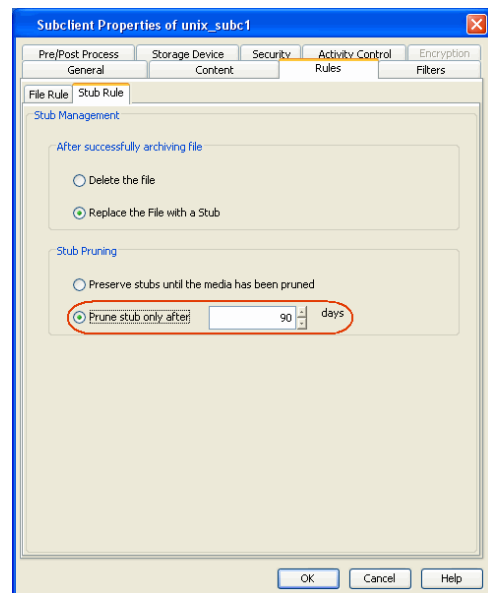
CONFIGURING FOR OPTIMIZED STUB RECALL

EXTEND THE PERSISTENT PIPELINE TIMEOUT

It is recommended to leave the persistent pipeline open for longer periods of time to cache important information for subsequent recall attempts. By default this timeout is set to 24 hours.

1. From the CommCell Browser, right-click the client computer that has Unix Archiver Agent installed.

2. Click **Properties**.

3. Select **Registry Key Settings**.

4. Click **Add**.

5. Enter `nDMRSIDLETIMEOUT` in the **Name** field.

6. Enter `EventManager` in the **Location** field.

7. From the **Type** list, select REG_DWORD.

8. Enter the number of seconds after which the pipeline will close. The valid range is 0 to 2147483647 seconds.

9. Click **OK**.

Once this key is activated, services must be restarted on the client computer.
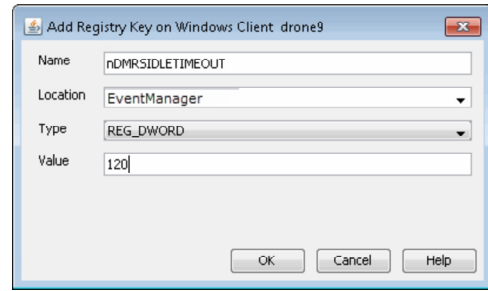
LIMIT THE NUMBER OF PERSISTENT PIPELINE THREADS DURING RECOVERIES

You can increase the number of persistent pipeline threads allowed for recoveries, thereby potentially improving stub recall speed. The recommended number of threads would be the number of Media Agents, which could possibly be used for recoveries. By default two threads will be used. Therefore if more than two Media Agents are potential targets for stub recalls increase the number of threads accordingly as follows:

1. From the CommCell Browser, right-click the client computer that has Unix Archiver Agent installed.

2. Click **Properties**.

3. Select **Registry Key Settings**.

4. Click **Add**.

5. Enter nDMRMaxRestoreThreads in the **Name** field.

6. Enter EventManager in the **Location** field.

7. From the **Type** list, select REG_DWORD.

8. Enter the number of persistent pipelines to be allowed.

9. Click **OK**.
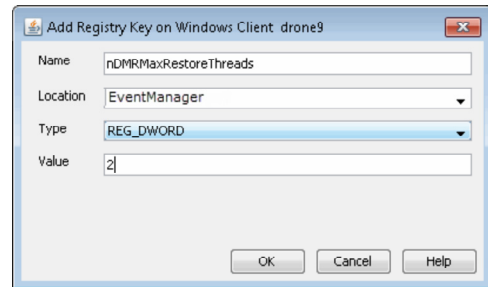
Once this key is activated, services must be restarted on the client computer.

STUB RECALL FROM ANY AVAILABLE DATA COPY

By default if the primary copy of the data is unavailable the stub recall will fail. However you can configure to trigger stub recall from an alternate data copy as follows:

1. In the Comcell Browser double-click the **Control Panel**.

2. Click the **Browse/Search/Recovery** option.

3. Select the **Automatically switch copy to read data from any copy** option.

4. Click **Ok**.
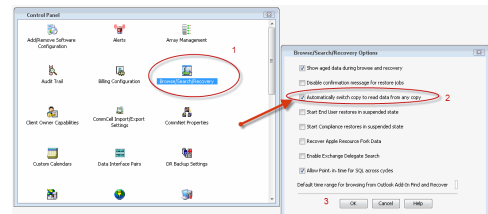
FILTERING FILES FROM ARCHIVING

Prior to archiving the files, you can set filters to prevent specific type of files from being archived. Filters can also be used to exclude certain system-related files and database application files which consistently fail during a archive operation and are not integral to the operation of the system or application.

FILES EXCLUDED FROM ARCHIVING

Files with extensions *.a, *.ksh, *.csh, *.sh, *.lib, and *.so are automatically filtered out of subclient content by default. Similarly, files in the following directories are also skipped from archiving on all Unix platforms.

- /usr/**
- /bin/**
- /lib/**
- /boot/**
- /dev/**
- /etc/**
- /var/**
- /tmp/**

- /sbin/**

- /lib64/**

- /opt/**

- /sys/**

- /kernel/**

- /devices/**

- /proc/**

- /selinux/**

- /stand/**

MANUALLY FILTERING FILES FROM ARCHIVING

You can manually set filters on selected file types, folders or files to be excluded from archiving. For example if you specify *.txt in the filters then all the text files will be excluded from being archived.

1. **Client Computers | <Client> | File Archiver | Instance | ArchiveSet.**

2. In the right pane right-click the **Subclient** and click **Properties**.

3. Click the **Filters** tab.

4. Click **Add** from the **Exclude these files/folders/patterns** group.

5. Enter the complete path of the file, folder, or directory that you want to exclude from the archiving operations

    or

    Click the **Browse** and expand the file system of the client computer. Click the file, folder, or directory that you want to exclude from the archiving operations and then click **Add**.

6. Click **OK** to save your changes.
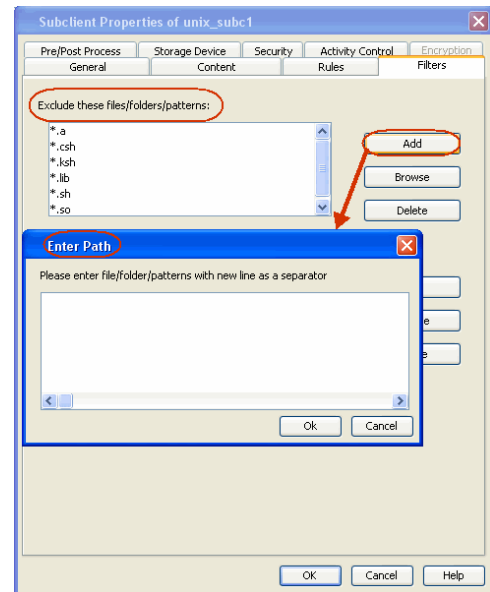
MANUALLY INCLUDING FILES FOR ARCHIVING

When excluding files from archiving, you can also provide exceptions to the data that you are excluding. For example, if you want to exclude from your migration archive operation all the files in the /Ops directory except the Maintenance file, you can add a subclient filter to exclude the /Ops directory from being archived and also add a corresponding subclient filter to allow the Maintenance file to be archived.

1. **Client Computers | <Client> | File Archiver | Instance | ArchiveSet.**

2. In the right pane right-click the **Subclient** and click **Properties**.

3. Click the **Filters** tab.

4. Click **Add** from the **Include these files/folder/patters:** group.

5. Enter the complete path of the file, folder, or directory that you want to be included in the archiving operation.

    or

    Click the **Browse** and expand the file system of the client computer. Click the file, folder, or directory that you want to be included in the archiving operation. and then click **Add**.

6. Click **OK**.

CONFIGURING THE MAXIMUM NUMBER OF SIMULTANEOUS STUB RECALLS (RECALL THROTTLING)

The maximum number of simultaneous stub recalls can be limited to a specified amount of time. This will not only optimize performance but can also prevent the inadvertent recovery of a large number of files.

1. From the CommCell Console, navigate to **Client Computers | <Client>.**

2. Right-click **File Archiver.**

3. Select **Properties**.

4. Click **Stub Recovery Parameters**.

5. In the **Maximum Stub Recovery** box select a value.

6. In the **Time between recall to count as successive in seconds** box select a value.

7. In the **Time to wait after maximum successive recalls limit is reached in seconds** box select a value.

8. Click **OK**.

   It might take some time for the changes to take effect. Restart the File Archiver services for it to take effect immediately.

CONFIGURING ARCHIVING FOR X9000 IBRIX

For X9000 IBRIX , by default the stubs are recalled during the data tiering process, which moves the files and the data stubs from one storage tier to another based on pre determined parameters. However you can configure the sTranProcName registry key to seamlessly migrate data stubs from one storage tier to another without triggering a stub recall. The steps to configure the key are as follows:

1. From the CommCell Browser, navigate to **Client Computers**.

2. Right-click the <*Client*> and then click **Properties**.

3. Click the **Registry Key Settings** tab.

4. Click **Add**.

5. In the **Name** field, type sTranProcName

6. In the **Location** list, type or select `UnixFsDataMigrator`.

7. In the **Type** list, select **Value**.

8. In the **Value** field, type the process name used migrate stubs from one storage tier to another.

   Example migrator_daemon

   On specifying this value the stubs will not be recalled during the data tiering process.

9. Click **OK**.
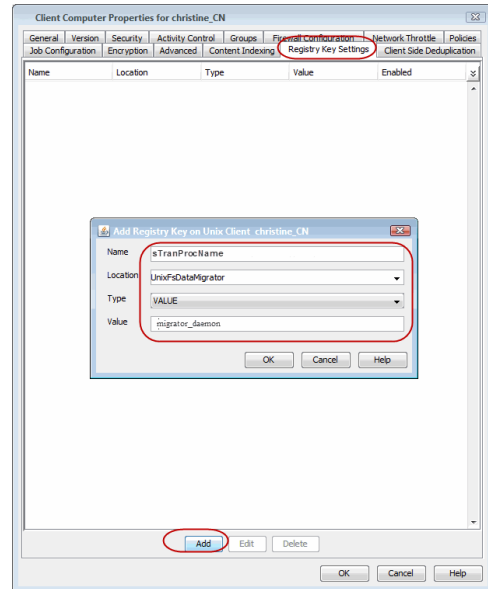
CONFIGURING ARCHIVING FOR LUSTRE FILE SYSTEM

Perform the following to configure archiving for Lustre file system:

1. Mount the Lustre file system on all the nodes. By default the File Locks are not enabled for Lustre.

    In order to archive the files using the archiver agent, mount the file system with -o flock or localflock option.

    For example [root@LustreClient01 ~]# mount –t lustre –o flock lustre192.168.0.10@tcp0:/lustre /mnt/lustre

2. From the CommCell Browser, navigate to **<Client> | File System | Default Backup Set**.

3. Right-click **Default Backup Set | All Tasks**

4. Click **New Subclient**.

5. In the General tab enter **Subclient Name**.

6. Click the **Content** tab.

7. Click **Add Paths** to add the mount point created in **Step 1** as the subclient content.

8. Click the **Storage Device** tab.

9. Select the **Storage Policy** from the drop down list.

10. Click **OK**.

    Repeat the above mentioned procedure for all the nodes of the clustered file system.
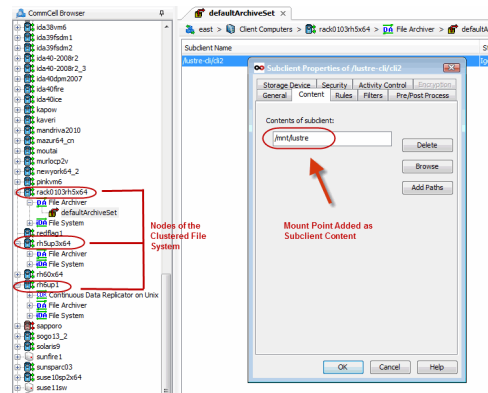
SETTING UP STUB CACHE

After recalling the files, you can re-archive the recalled files by preserving them in a stub cache. The recalled file will be re-archived from the cache if the file meets the archiving rules and has not been modified after the recall. The following registry keys allow you to set the stub cache and re-stub the recalled files from the cache memory.

nUSE_STUB_CACHE	This key allows a file to be re-stubbed after recall by preserving it in cache memory.
dSTUB_CACHE_ROOT	By default the stubs are cached under , /opt/calypso/stubcache folder. Use this key to specify a different location of the root folder for the File Archiver stub cache.

MODIFYING AN ARCHIVESET OR SUBCLIENT

The following table describes the properties that can configured from the agent, backup set/archive set, and subclient levels.

OPTION	DESCRIPTION	RELATED TOPICS
Configure Activity Control	You can enable backup and restore operations from the agent and subclient level. However, you can enable recovery operations only from the agent level. Agent Level: 1. From the CommCell browser, right-click the File Archiver Agent. 2. Click **Properties**. 3. Click **Activity Control**, select or clear **Enable Archive** and **Enable recovery** options. 4. Click **OK.** Subclient Level: 1. From the CommCell browser, right-click the subclient. 2. Click **Properties**. 3. Click **Activity Control**, select or clear **Enable Archive** option. 4. Click **OK.**	Refer to Activity Control.
Release License	You can release a license for client, MediaAgent and agent. If releasing a license is successful, the tree element is dimmed and available for deletion. 1. From the CommCell browser, right-click the **File Archiver Agent**. 2. Click **All Tasks** and select **Release License**. 3. Click **OK** to continue. 4. Click **Yes** to continue with the deconfiguration or **No** to abort.	
Change Storage Policies	You can modify the storage policies in any of the following situations. ● To include a different media for the backup operation. ● To use a storage policy with a different retention criteria. You can change the storage policies from the subclient level. 1. From the CommCell Browser, right-click the subclient. 2. Click **Properties**. 3. Click **Storage Device** tab. 4. Click **Data Storage Policy** tab and select a data storage policy to associate with this subclient. 5. Click **OK** to save your settings.	Refer to Storage Policies.
Rename Backup Set/Archive Set	You can rename an existing Backup Set/Archive Set. 1. From the CommCell Browser, right-click the Backup Set/Archive Set. 2. **C**lick **Properties.** 3. Click **General** tab and type the new name in the Backup Set field. 4. Click **OK** to save your settings.	
Rename a Subclient	You can rename an existing subclient. 1. From the CommCell Browser, right-click the subclient. 2. **C**lick **Properties.** 3. Click **General** tab and type the new name in the **Subclient Name** field 4. Click **OK** to save your settings.	
Configure Data Transfer Options	You can efficiently configure the available resources for transferring data secured by data protection operations from the subclient level. This includes the following: ● Enable or disable **Data Compression** either on the client or the MediaAgent. ● Configure the transfer of data in the network using the options for **Network Bandwidth Throttling** and **Network Agents**. You can configure the data transfer options. 1. From the CommCell Browser, right-click the subclient. 2. Click **Properties.** 3. Click **Storage Device.** 4. Click **Data Transfer Option** tab. 5. Choose the appropriate software compression option for this subclient. 6. Select **Throttle Network Bandwidth** and set the required bandwidth. 7. Click **OK.**	Refer to Data Compression and Network Bandwidth Throttling.
View Data Paths	You can view the data paths associated with the primary storage policy copy of the selected storage policy or incremental storage policy. You can also modify the data paths including their priority from the subclient level.	

	1. From the CommCell browser, right-click the subclient.	
	2. Click **Properties.**	
	3. Click **Storage Device.**	
	4. Select **Storage Policy** from the drop-down menu.	
	5. Click **Data Paths.**	
Configure account for Pre/Post Processing of Data Protection	You can add, modify or view Pre/Post processes for the subclient. These are batch files or shell scripts that you can run before or after certain job phases.	Refer to Pre/Post Processes.
	1. From the CommCell browser, right-click the subclient.	
	2. Click **Properties**.	
	3. Click **Pre/Post Process**.	

	4. Click one of the following phases and type the full path of the process that you want to execute during that phase. Alternatively, click **Browse** to locate the process (applicable only for paths that do not contain any spaces).
	  ○ **PreBackup Process**
	  ○ **PostBackup Process**	

	5. Click **OK**.	
	6. Select **Run Post Scan Process for all attempts** to run a post scan process for all attempts .	
	7. Select **Run Post Backup Process for all attempts** to run a post backup process for all attempts.	

	8. For subclients on Windows platforms, **Run As** displays **Not Selected**.
	
	If you want to change the account that has permission to run these commands, click **Change**.
	
	  a. In the **User Account** dialog box, select **Use Local System Account,** or select **Impersonate User** and enter the user name and password. Click **OK**.
	
	  b. If you selected Local System Account, click **OK** to the message advising you that commands using this account have rights to access all data on the client computer.	

Configure User Security	You can configure user security from the agent, backup set/archive set or subclient levels. You can perform the following functions: ● Identify the user groups to which this CommCell object is associated. ● Associate this object with a user group. ● Disassociate this object from a user group.	Refer to User Administration and Security.
	1. From the CommCell browser, right-click the subclient.	
	2. Click **Properties**.	
	3. Click **Security**.	
	4. Select the appropriate user groups to which you want to associate to the CommCell object from the **Available Groups** pane, and then move the user group to the **Associated Groups** pane.	
	5. Click **OK**.	
Enable/Disable Data Encryption	You must export the pass-phrase to the local computer before performing a stub recovery operation of encrypted data. You can enable data encryption from the subclient level. Encryption must be enabled at the client level prior to configuring any instances residing on that client.	Refer to Data Encryption.
	1. From the CommCell browser, right-click the subclient.	
	2. Click **Properties.**	
	3. Click **Encryption.**	
	4. Select the desired encryption.	
	5. Click **OK**.	
View Software Version and Installed Updates	The **Version** tab, at the Agent level displays the software version and post-release service packs and updates installed for the component.	
	1. From the CommCell browser, right-click the agent.	
	2. Click **Properties**.	
	3. Click **Version**.	
	4. Click **OK**.	
CommCell Configuration Report	The CommCell Configuration Report provides the properties of the CommServe, MediaAgents, clients, agents, SRM agents, subclients, and storage policies within the CommCell based on the selected filter criteria.	Refer to CommCell Configuration.
	1. From the CommCell browser, click **Reports** icon.	

	2. Select **CommCell Configuration**.	
	3. Click **Run**.	
Archive Job Summary Report	The Archive Job Summary Report provides the detailed archive information such as the start and end time (or current phase), the total size of the archive job, the elapsed time, the transfer time, the throughput, the number of objects archived, the amount of data, the failed folders and files, content indexing usage and failures (if any), and the filters used for the archive. 1. From the CommCell browser, click **Reports** icon. 2. Select **Job Summary**. 3. Click **General** and select **Archive/Compliance Archive.** 4. Click **Run**.	Refer to Archive/Compliance Archive Job Summary Report

DELETING AN AGENT, ARCHIVESET OR SUBCLIENT

The following sections describe the steps involved in deleting an agent, archive set or subclient.

When you delete an instance or backupset, the associated data is logically deleted and you can no longer access the corresponding data from CommCell Console for recovery purposes.

Refer to the troubleshooting article on Recovering Data Associated with Deleted Clients and Storage Policies for information on how to recover data if you accidentally delete an entity.

DELETING AN AGENT

You need to uninstall or DeConfigure the agent software from the client computer before deleting from CommCell Browser. After you delete the client software, you can either leave the corresponding data intact for appropriate action or you can remove the data immediately. If you choose to remove the data immediately, you must delete the agent from the CommCell Browser. If you delete the agent, all of the agent's data is irretrievably lost.

● You cannot delete an agent while operations for that agent are running.

1. From the CommCell Browser, navigate to **Client Computers | <Client>***.*

2. Right-click the **<Agent>***,* and then click **Delete**.

3. A confirmation message is displayed with the following message:

   This operation will permanently delete the data backed up from this level and it cannot be restored.

4. Click **OK** to continue with the deletion operation., or click **No** to abort the deletion.

DELETING A BACKUPSET/ARCHIVESET

Consider the following before deleting a Backup Set:

● You cannot delete a default Backup Set.

● Schedules associated with the Backup Set are also automatically deleted.

1. From the CommCell Browser, navigate to **Client Computers | <Client> | <Agent>.**

2. Right-click the **<Backup Set>**, and then click **Delete**.

3. A confirmation message is displayed, asking if you want to delete the Backup Set.

   Click **No** to cancel the deletion and retain the Backupset, or click **Yes** to continue the deletion.

DELETING A SUBCLIENT

Consider the following before deleting a subclient:

● You cannot delete a default subclient.

● Schedules associated with the subclient are also automatically deleted.

1. From the CommCell Browser, navigate to **Client Computers | <Client> | <Agent> | <Backup Set>.**

2. Right-click the **<subclient>** that you want to delete, and then click **Delete**.

3. A confirmation message is displayed, asking if you want to delete the subclient.

   Click **No** to cancel the deletion and retain the subclient, or click **Yes** to continue the deletion.

Back to Top

Advanced Archiving - File Archiver

TABLE OF CONTENTS

SCHEDULING AN ARCHIVE JOB

1.
- From the CommCell Console, navigate to **Client Computers** | **File Archiver | ArchiveSet**
- Right-click the **Subclient** in the left pane and click **Archive**.
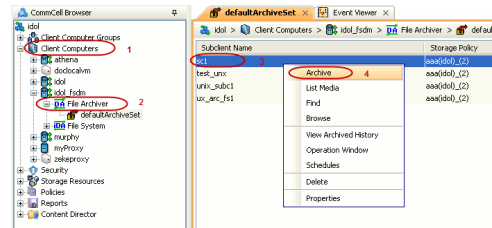
2.
- Click **Schedule** to schedule the archive job for a specific time.
- Click **Configure** to set the schedule for the archive job.
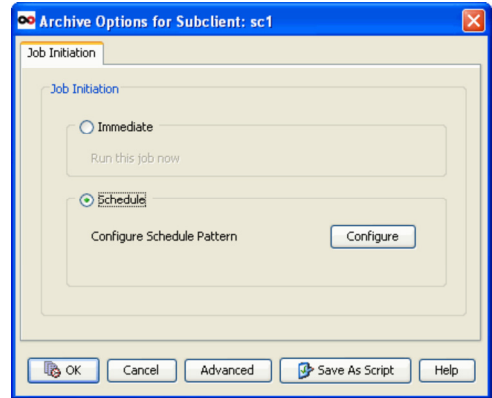
3.   In the **Schedule Details** dialog box select the appropriate scheduling options.

For example:
- Click **Weekly**.
- Check the days you want the run the archive job.
- Change the Start Time to 9:00 PM
- Click **OK** to close the Schedule Details dialog
- Click **OK** to close the Archive Options dialog

The archive job will execute as per the schedule.
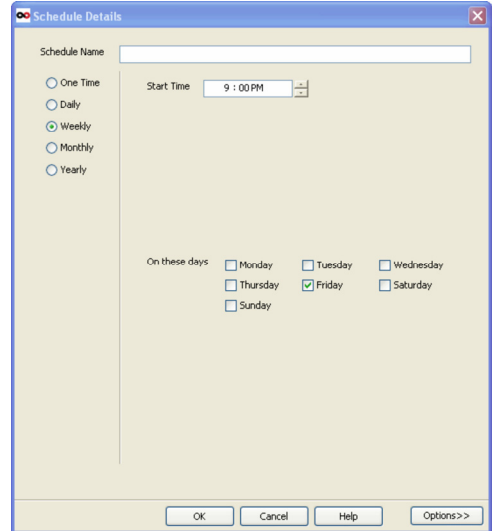
PREVIEWING FILES ELIGIBLE FOR ARCHIVING

By default running an archive job will archive and stub the files satisfying the pre-determined archiving criteria. However you can also view the files eligible for stubbing before running the archive job by following the steps given below:

1. On the Client computer navigate to the **tmp** folder and create the following file:

   /tmp/GXHSMIfind.dryrun

2. From the CommCell Console, navigate to **Client Computer** | **File Archiver** | **ArchiveSet**.

3. Right-click the **Subclient** and click **Archive**.

4. Select **Immediate** to run the job immediately.

5. Click **OK**.

6. On the Client computer navigate to the **/tmp/GXHSMIfind.collect** and verify that the GXHSMIfind.collect file contains the names of all the files that will be stubbed.

7. Remove the **GXHSMIfind.dryrun** file and rerun the Archive job from the ComCell Console.

PROTECTING STUBS IN BACKUPS

DURING FULL BACKUP

These stubs are normally included and protected in full backup operations by the Unix file system *i*DataAgent.

DURING INCREMENTAL BACKUP

Stubs are not included by default in Incremental Backups when the Classic Scan method is used to scan files. This means that stubs created after the most recent full backup may be lost if the operating system or file structure where the stubs reside is destroyed or rendered unusable before the next full backup is run. However, the archived data is still recoverable through a browse recovery operation from the CommCell Console.

*i*DataAgents can be configured to include stubs in Incremental Backups (and in turn Synthetic Full Backups) so that stubs are not lost. Stubs can be included in Incremental Backups as follows:

● Enable the **Check Archive Bit During Backups** option on the backup set of the associated File System *i*DataAgent prior to running the incremental backup.

● Enable the **Use Change Journal** or **Use Data Classification** option on the backup set of the associated File System *i*DataAgent prior to running the incremental backup.

● Set the `ifindUseMTime` registry key value to N in the properties file on the client computer.

RE-STUBBING A FILE IMMEDIATELY AFTER A RECALL

The nUSE_STUB_CACHE key allows a file to be re-stubbed immediately after recall by preserving it in cache memory.

MANAGING JOBS

Jobs can be managed in a number of ways. The following sections provide information on the different job management options available:

RESTARTING JOBS

Jobs that fail to complete successfully are automatically restarted based on the job restartability configuration set in the Control Panel. Keep in mind that changes made to this configuration will affect all jobs in the entire CommCell.

To Configure the job restartability for a specific job, you can modify the retry settings for the job. This will override the setting in the Control Panel. It is also possible to override the default CommServe configuration for individual jobs by configuring retry settings when initiating the job. This configuration, however, will apply only to the specific job.

Backup jobs for this Agent are resumed from the point-of-failure.

CONFIGURE JOB RESTARTABILITY AT THE COMMSERVE LEVEL

1. From the CommCell Browser, click **Control Panel** icon.

2. Select **Job Management.**

3. Click **Job Restarts** tab and select a **Job Type.**
   ○ Select **Restartable** to make the job restartable.
   ○ Change the value for **Max Restarts** to change the maximum number of times the Job Manager will try to restart a job.

o Change the value for **Restart Interval (Mins)** to change the time interval between attempts for the Job Manager to restart the job.

4. Click **OK.**
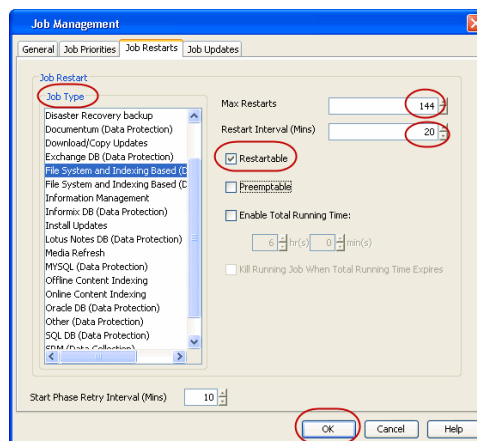
CONFIGURE JOB RESTARTABILITY FOR AN INDIVIDUAL JOB

1. From the CommCell Console, navigate to **<*Client*>** | **File Archiver** | **<*Instance*>**

2. Right-click the **Subclient** and select **Archive**

3. Click **Advanced.**

4. In the **Advanced Backup Options** dialog box, click the **Job Retry** tab.

5. Select **Enable Total Running Time** and specify the maximum elapsed time before a job can be restarted or killed.

   Select **Kill Running Jobs When Total Running Time Expires** to kill the job after reaching the maximum elapsed time.

6. Select **Enable Number Of Retries** and specify the number of retries.

7. Click **OK.**
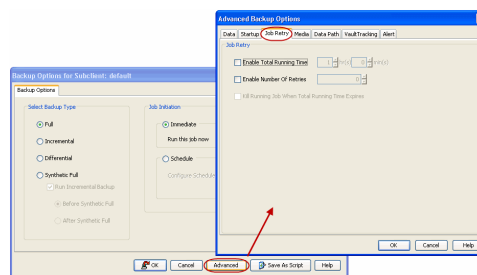
CONTROLLING JOBS

The following controls are available for running jobs in the Job Controller window:

SUSPEND	Temporarily stops a job. A suspended job is not terminated; it can be restarted at a later time.
RESUME	Resumes a job and returns the status to Waiting, Pending, Queued, or Running. The status depends on the availability of resources, the state of the Operation Windows, or the Activity Control setting.
KILL	Terminates a job.

SUSPENDING A JOB

1. From the Job Controller of the CommCell Console, right-click the job and select **Suspend**.

2. The job status may change to **Suspend Pending** for a few moments while the operation completes. The job status then changes to **Suspended.**

RESUMING A JOB

1. From the Job Controller of the CommCell Console, right-click the job and select **Resume**.

2. As the Job Manager attempts to restart the job, the job status changes to **Waiting**, **Pending**, or **Running**.

KILLING A JOB

1. From the Job Controller of the CommCell Console, right-click the job and select **Kill**.

2. Click **Yes** when the confirmation prompt appears if you are sure you want to kill the job. The job status may change to **Kill Pending** for a few moments while the operation completes. Once completed, the job status will change to **Killed** and it will be removed from the Job Controller window after five minutes.

JOB RESULTS PATH

Archived files will not get stubbed when the job results path is an UNC path**.** Therefore, it is recommended to save job results in a local file such as the default path as opposed to specifying the UNC path.

ADDITIONAL OPTIONS

Several additional options are available to further refine your Archiving operations. The following table describes these options, as well as the steps for configuring them.

Be sure to read the overview material referenced for each feature prior to using them.

OPTION	DESCRIPTION	RELATED TOPICS
Data	You can select advanced backup/archive data options for the archive operation. 1. From the CommCell Browser,click **Client Computers | File Archiver | ArchiveSet**.The default and other subclients (if available) are displayed on the right-hand window pane. 2. Right-click the subclient that contains the data you want to archive. 3. Click **Archive**. 4. Click **Advanced.** ○ Check the option **Create new Index** to create a new index with a full or On Demand data protection operation. 5. Select the desired Catalog option for index cache sharing and granular restartability options for the job.	
Startup	You can select advanced backup/archive data options for the operation. 1. From the CommCell Browser, click **Client Computers | File Archiver | ArchiveSet**. The default and other subclients (if available) are displayed on the right-hand window pane. 2. Right-click the subclient that contains the data you want to archive. 3. Click **Archive**. 4. Click **Advanced**. 5. Click **Startup**. 6. Select Use **Default Priority** option to use default priority for the job. ○ Select **Change priority** option to change the priority for a job, between 0 (highest priority) and 999 (lowest priority). 7. Select **Start up in Suspended State** option to specify the selected job to start in the Job Controller in a suspended state. 8. Click **OK.**	Refer to Job Priority and Priority Precedence.
Job Retry	The Archive jobs can be restarted either by a user or automatically by the Job Manager. You can specify the maximum elapsed time before a job can be restarted or killed and the maximum number of restart attempts. 1. From the CommCell Browser, click **Client Computers | File Archiver | ArchiveSet**. The default and other subclients (if available) are displayed on the right-hand window pane. 2. Rght-click the subclient that contains the data you want to archive. 3. Click **Archive.** 4. Click **Job Retry.** 5. Select **Enable Total Running Time**. 6. Select **Enable Number of Retries** option to select number of times the Job Manager will attempt to restart the job. 7. Select **Kill Running Jobs When Total Running Time Expires** option to kill the job when the specified Total Running Time has elapsed. 8. Click **OK**.	Refer to Job Management for more information

Media	You can select the advanced archive media options for the archive operation.
	
	1. From the CommCell Browser, click **Client Computers | File Archiver | ArchiveSet**. The default and other subclients (if available) are displayed on the right-hand window pane.
	
	2. Right-click the subclient that contains the data you want to archive.
	
	3. Click **Archive**.
	
	4. Click **Advanced**.
	
	5. Click **Media**.
	
	6. Select **Start New Media** to start archive operation on a new media.
	
	7. Select **Mark Media Full on Success** to mark this media full after the completion of the archive operation.
	
	8. Select **Reserve Resources Before Scan** to reserve the media before the scan phase.
	
	9. Select **Infinite** under Extend Job Retention to retain this job indefinitely.
	   ○ Select **Number of Days** to specify the number of days after which this job will be pruned.
	   ○ Select **Storage Policy Default** to apply the retention rules of the associated storage	

	policy. 10. Click **OK**.	
Data Path	Data Protection operations use a specific data path (Library, MediaAgent, Drive Pool, and Drive) to perform the backup operations as configured in the CommCell. By default, the system automatically identifies the data path for the backup operations. The following are some of the important situations where you may need to change the data path: ● When the preferred MediaAgent, library or drive pool is not available during the backup ● When you need to use a different MediaAgent, library or drive pool for load balancing purposes. ● When you need to direct that backup to a particular location for compliance purposes. 1. Right-click the Subclient and select **Archive**. 2. From the **Archive Options** for Subclient window, click **Advanced**. 3. From the **Data Path** tab, select **Use MediaAgent** and **Use Library** or **Use Drive Pool** and **Use Drive** from the respective drop-down combo boxes. 4. Click **OK**.	Refer Change Data Path for more information.
Vault Tracking	The VaultTracker feature provides the facility to manage media that are removed from a library and stored in offsite locations. 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. ● Identifies and tracks the media during transit. ● Records and tracks the movement of media not used by all MediaAgents or Foreign Media. 1. Right-click the Subclient and select **Archive**. 2. From the **Archive Options for Subclient** window, click **Advanced**. 3. From the **VaultTracking** tab, select the necessary options. 4. Click **Ok**.	Refer to the following documentation for a comprehensive overview prior to using this feature: ● VaultTracker if a standard CommServe license is available. ● VaultTracker Enterprise if the VaultTracker Enterprise license is available.
Alert	The Alert option is used for setting up the criteria to raise notifications/alerts for job statuses such as failure, success, or any other conditions triggered by the backup job. Adding alerts helps the user or the user group to get the notification automatically about the status of the backup job. 1. Right-click the Subclient and select **Archive**. 2. On the **Archive Options for Subclient** window, click **Advanced**. 3. On the **Alert** tab, click **Add Alert** and it opens **Add Alert Wizard** window. 4. From the **Add Alert Wizard** window, select the **Threshold and Notification Criteria**. Click **Next**. 5. Select the **Notification Types**. Click **Next**. 6. Select the **Users and User Groups**. Click **Next**. 7. Click **Finish**.	Refer Alerts for more information.

Advanced Recovery - File Archiver

TABLE OF CONTENTS

RECOVER DATA FROM COMMCELL CONSOLE

Use the following method to restore stubs. Deleted stubs that are not yet aged, can also be recovered by performing a Browse and Restore.

1. From the CommCell Console, navigate to **<Client>** | **File System**.

2. Right-click the archive set that contains the data you want to restore and click **All Tasks** | **Browse Backup Data**.

3. Click **OK**.

4. Select the folder level under the backup set. Its entire contents will be automatically selected in the right pane.

5. Click **Recover All Selected**.

6. From the **General** tab, either specify **Recover to Same Paths** or **Specify destination path** by typing a path or clicking **Browse** to locate the desired destination.

7. Click the **Job Initiation** tab.

8. Select **Immediate** to run the job immediately.

9. Click **OK**.

10. You can monitor the progress of the restore job in the **Job Controller** or **Event Viewer** window of the CommCell Console.

11. This will restore stubs in the specified destination.

12. To restore data, navigate to the location the stubs are restored and perform a stub recovery.
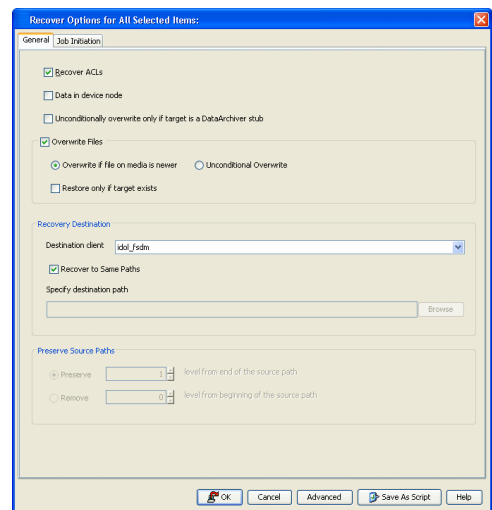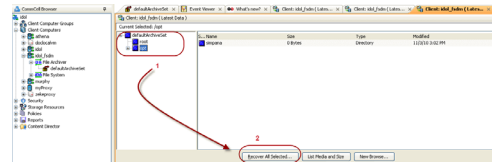
MOVING STUBS

If a stub has been moved to a new location, recall operations will recover data to the new location and not the originating one.

- If stubs are moved within the monitored volume, it does not trigger a stub recall and the file is moved.
- If stubs are moved outside the monitored volume, it triggers a stub recall and the file is moved.

For example, moving files using the `mv` command:

1. Open a Terminal or Console Window.

2. Move a single file or use wildcards to move multiple files.

    `mv` *<filename> <new path>*

    `mv` *<*.pdf> <new path>*

COPYING STUBS

If stubs are copied within or outside the monitored volume, it triggers a stub recall.

For example, copying files using the `cp` command:

1. Open a Terminal or Console Window.

2. Copy a file to another location.

    `cp` *<filename> <new path>*

ACCESSING STUBS WITHOUT TRIGGERING A RECALL

Stubs can be accessed without triggering a recall, by using the Registry key sTranProcName.

SCHEDULING A RESTORE

1.
- From the CommCell Console, navigate to **Client Computers** | **File Archiver**.
- Right-click an archive set and click **All Tasks** | **Browse**.
- Click **OK**.

2.
- Select data to restore.
- Click **Recover All Selected**.

3.
- Click **Job Initiation** tab and click **Schedule**.
- Click **Configure**.
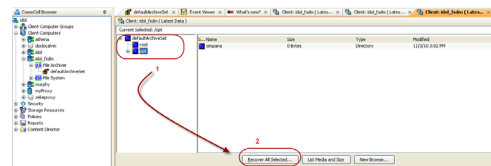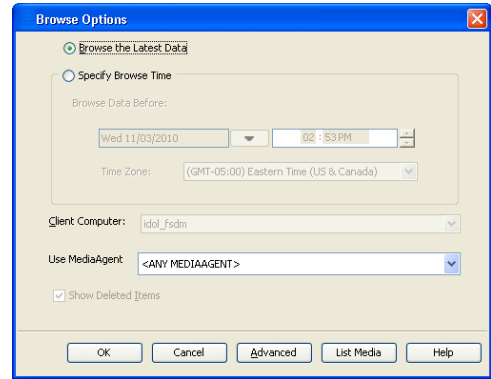
4. Select the appropriate scheduling options. For example:
- Click **Weekly**.
- Check the days you want the run the restore job.
- Change the Start Time to 9:00 PM
- Click **OK** to close the Schedule Details dialog
- Click **OK** to close the Restore Options dialog

The restore job will execute as per the schedule.
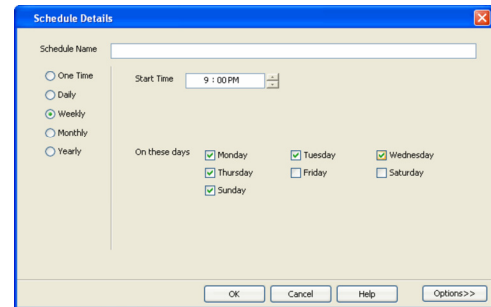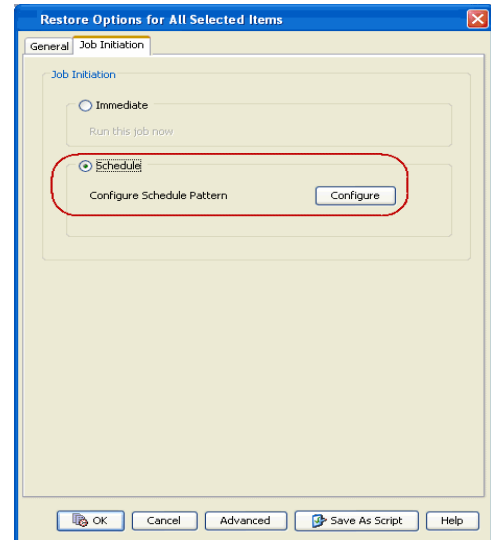
RESTORE DESTINATIONS

By default, the File Archiver for Unix restores data to the client computer from which it originated; this is referred to as an in-place restore. You can also restore the data to another client computer in the CommCell. The following section enumerates the types of restore destinations that are supported by the File Archiver for Unix.

IN-PLACE RESTORE

When restoring data, the File Archiver for Unix provides the facility to restore the data to the same path/destination on the client computer from which the data originated; this is referred to as an in-place restore.

1. From the CommCell Console, perform a **Browse and Restore** operation.

2. When browsing the data, select data that was initially backed up and click **Recover All Selected**.

3. Click **OK**.

4. Select the **Destination Client** that was the original computer from which the data originated.

5. Depending on the data selected to restore, choose one of more of the options (e.g., **Restore ACLs**).

6. Click **OK**.

OUT-OF-PLACE RESTORE

All restore levels provide the facility to restore data to a different directory on the client computer from which the data originated; this is referred to as an out-of-place restore to a different path/destination. You can also restore data to a different client computer in the CommCell using the same path/destination.

Keep in mind the following considerations when performing out-of-place restores:
- The destination client must reside in the same CommCell as the client whose data was backed up.
- Note that when you perform an out-of-place restore, the restored data assumes the rights (i.e., permissions) of the parent directory.

1. From the CommCell Console, perform a **Browse and Restore** operation.

2. When browsing the data, select data that was initially backed up and click **Recover All Selected**.

3. Click **OK**.

4. Select the **Destination Client** that is a different computer from which the data originated.

5. Depending on the data selected to restore, choose one of more of the options (e.g., **Restore ACLs**).

6. Click **OK**.

RESTORING TO AN NFS MOUNTED FILE SYSTEM

Besides recovering data to a client computer's local drive, you can also recover data to a NFS-mounted file system.

Ensure that the destination computer has root permissions for the NFS-mounted file system. If the destination computer does not have these permissions, restores will fail.

1. From the CommCell Console, perform a **Browse and Restore** operation.

2. When browsing the data, select data that was initially backed up and click **Recover All Selected**.

3. Click **OK**.

4. Select the **Destination Client** on which to restore the data.

5. Deselect **Recover to Same Paths**.

6. In Specify destination path, enter the NFS mounted file system or click **Browse**.

7. Click **OK**.
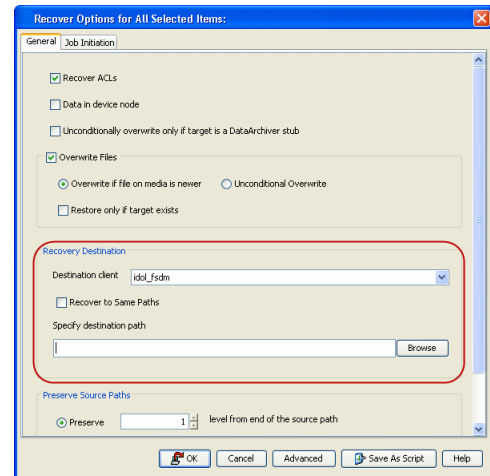
RESTORING BY JOBS

The Restore By Jobs feature provides the facility to select a specific backup job to be restored. This method of restoring data is considerably faster as it reads continuously on the tape and retrieves the data and does not depend on the indexing subsystem to get the seek offsets on the media.

This feature can be used in different scenarios such as the following:

● To restore point-in-time data associated with a specific backup job, such as full, incremental, differential, etc.

● To restore CommServe DR data for the disaster recovery or for creating a hot-site purposes.

● To restore multiplexed data from the same client.

Consider the following when restoring by jobs:

● Run a restore by jobs whenever you want to restore the entire contents of the job.

● Avoid running restores by jobs for jobs associated with the default subclient. If you do this, the entire contents of the machine will be restored. As such, this may cause problems (e.g., the machine might run out of space) or produce undesirable results (e.g., you might end up restoring operating system files or directories that you really do not want to restore).

● Avoid modifying the contents of any associated subclients since this may result in the retrieval of older data.

Use the following steps to restore data by jobs.

1. From the CommCell Browser, right-click the level whose data you want to browse, click **View** and then click the **Backup History**.

2. From the **Backup History Filter** window, select the filter options, if any, that you want to apply and click **OK**.
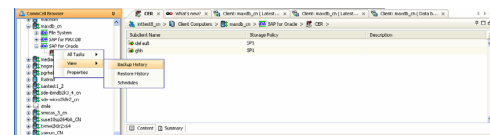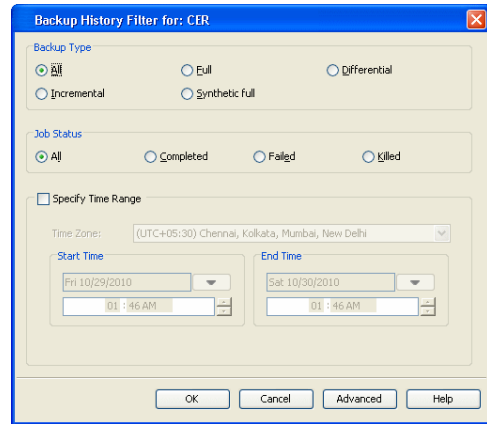
3. From the Backup Job History window, right-click the backup job that need to be restored and select **Browse**.

4. From the **Browse Options** dialog box, click **OK** to execute the browse using the **Browse the Latest Data** option.

5. From the **Browse** window, select the instance node in the left pane and then select the required data and logs in the right pane, and click the **Recover All Selected** button at the bottom of the window.

6. Select the desired restore options and click **OK**.

CONFIGURING THE MAXIMUM NUMBER OF SIMULTANEOUS STUB RECALLS (RECALL THROTTLING)

The maximum number of simultaneous stub recalls can be limited to a specified amount of time. This will not only optimize performance but can also prevent the inadvertent recovery of a large number of files.

1. From the CommCell Console, navigate to **Client Computers | <Client>.**

2. Right-click **File Archiver.**

3. Select **Properties**.

4. Click **Stub Recovery Parameters**.

5. In the **Maximum Stub Recovery** box select a value.

6. In the **Time between recall to count as successive in seconds** box select a value.

7. In the **Time to wait after maximum successive recalls limit is reached in seconds** box select a value.

8. Click **OK**.

   It might take some time for the changes to take effect. Restart the File Archiver services for it to take effect immediately.

FINDING AND RESTORE

BY NAME AND LOCATION

Use Find to locate files, directories, or objects from archived data. This option can be invoked from the agent, archive set, or subclient level.

1. From the CommCell Browser, navigate to **Client Computers | <Client> | File Archiver | Instance**.

2. Right-click **Archive Set** point to **All Tasks** and click **Find**.

3. In the **Name/Pattern** box enter the name of the file that you want to find.

4. In the **Folder** box browse and enter the path to the folder where the file might exists to narrow down the search.

5. Click **Search**.

6. Right-click the file in the right-pane and select one of the following:
   - **Restore** the file, folder or directory.
   - **Restore All Selected** files, folders or directories.
   - **View all Versions** of the selected file.
   - **Restore all Versions** of the selected file (not available for all agents).

7. Click **Ok**.

8. Select **Recover to Same Paths** box or in the **Specify destination path** box type the destination path or click **Browse** to locate the desired destination.

9. Click the **Job Initiation** tab.

10. Select **Immediate**.

11. Click **OK**.
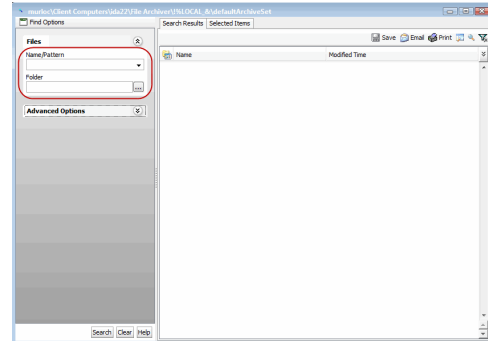
QUICK SEARCH USING SAMPLING

1. From the CommCell Browser, navigate to **Client Computers | <*Client*> | File Archiver | Instance**.

2. Right-click **Archive Set** point to **All Tasks** and click **Find**.

3. Click **Advanced Options** to expand and display the fields.

4. In **Sample Every,** specify the rate at which messages are sampled to determine whether they match the search criteria. The default value of 1 indicates that every message will be sampled. Keep in mind that the order in which messages are sampled is based on the order in which the messages were backed up.

5. Click **Search**.

6. Right-click the file in the right-pane and select one of the following:
   - **Restore** the file, folder or directory.
   - **Restore All Selected** files, folders or directories.
   - **View all Versions** of the selected file.
   - **Restore all Versions** of the selected file (not available for all agents).

7. Click **Ok**.

8. Select **Recover to Same Paths** box or in the **Specify destination path** box type the destination path or click **Browse** to locate the desired destination.

9. Click the **Job Initiation** tab.

10. Select **Immediate**.

11. Click **OK**.
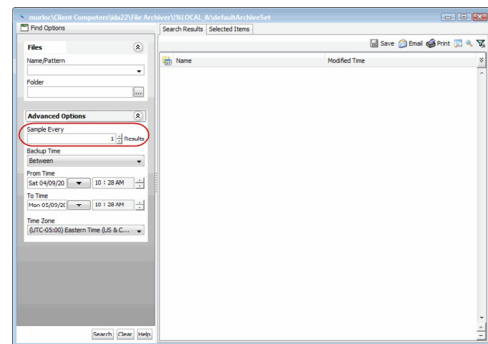
BY SPECIFIC TIME

1. From the CommCell Browser, navigate to **Client Computers | <*Client*> | File Archiver | Instance**.

2. Right-click **Archive Set** point to **All Tasks** and click **Find**.

3. In the **Name/Pattern** box enter the name of the file that you want to find.

4. In the **Folder** box browse and enter the path to the folder where the file might exists to narrow down the search.

5. Click **Advanced Options** to expand and display the fields.

6. In **Backup Time** box, specify a time or time range (Latest Cycle, After, Before, Between, Specific Date, Any, Today, Yesterday, This week, This Month, This Year, or Relative) to narrow searches to messages that were backed up within the time period specified.

7. Click **Search**.

8. Right-click the file in the right-pane and select one of the following:
   - **Restore** the file, folder or directory.
   - **Restore All Selected** files, folders or directories.
   - **View all Versions** of the selected file.
   - **Restore all Versions** of the selected file (not available for all agents).

9. Click **Ok**.
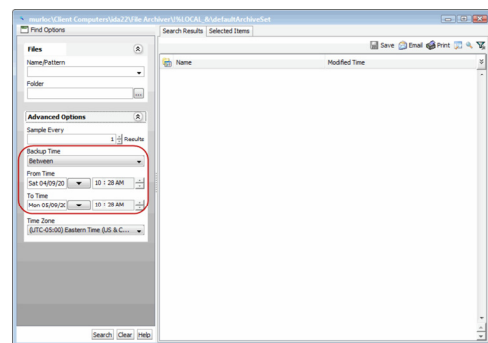
10. Select **Recover to Same Paths** box or in the **Specify destination path** box type the destination path or click **Browse** to locate the desired destination.

11. Click the **Job Initiation** tab.

12. Select **Immediate**.

13. Click **OK**.

LISTING MEDIA

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

The list media operation can be performed for instances, backup sets, and subclients. The following sections describe each of these methods.

The List Media feature can also be used in a number of other capacities. Refer to the List Media documentation for a complete overview of this feature.

LISTING 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.

LISTING MEDIA FOR AN ARCHIVE SET

1. From the CommCell Browser, right-click the archive set 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.

RESTORING ACLS

The ACLs and the data are restored by default when you restore data. You can choose to restore only the data or the ACLs and the data.

RESTORING THE ACLS AND DATA

Follow the steps given below to restore the ACLs and the data, and apply the ACLs to the data:

1. From the CommCell Console, navigate to **<Client>** | **File Archiver | Instance**.

2. Right-click Archive Set, point to **All Tasks** and click **Browse**.

3. Click **OK**.

4. Select the folder level under the backup set. Entire content will be automatically selected in the right pane.

5. Click **Recover All Selected**.

6. Select the **Restore ACLs** check box.

7. Click **OK**.
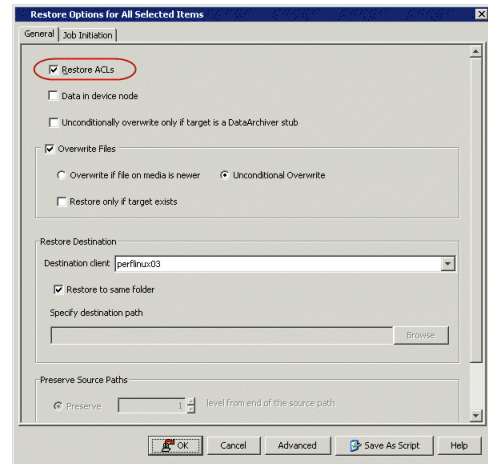
RESTORING ONLY DATA

You can restore only the data and inherit permissions from the parent directory in the destination. Follow the steps given below to restore only the data, without restoring the ACLs:

1. From the CommCell Console, navigate to *<Client>* | **File Archiver | Instance**.

2. Right-click Archive Set, point to **All Tasks** and click **Browse**.

3. Click **OK**.

4. Select the folder level under the backup set. Entire content will be automatically selected in the right pane.

5. Click **Recover All Selected**.

6. Click to clear the **Restore Data Only** check box.

7. Click **OK**.
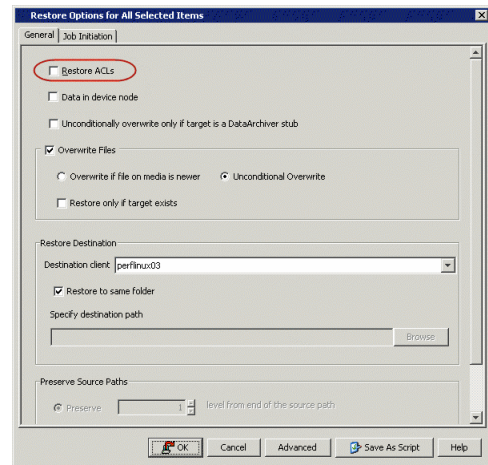
MANAGE RESTORE JOBS

Once you initiate the restore operation, a restore job is generated in the Job Controller. Jobs can be managed in a number of ways. The following sections provide information on the different job management options available:

RESTART JOBS

Jobs that fail to complete successfully are automatically restarted based on the job restartability configuration set in the Control Panel. This configuration can be changed at any time; however, changes to this configuration will affect all jobs run in the entire CommCell.

It is also possible to override the default CommServe configuration for individual jobs by configuring retry settings when initiating the job. This configuration, however, will apply only to the specific job.

Restore jobs for this Agent are re-started from the beginning.

CONFIGURE JOB RESTARTABILITY AT THE COMMSERVE LEVEL

1. In the CommCell Console, click the **Control Panel** icon, then double-click **Job Management**.

2. In the **Job Restarts** tab of the Job Management dialog box, select a job type from the **Job Type** list, and then select the **Restartable** check box.

3. To change the maximum number of times the Job Manager will try to restart a job, select a number in the **Max Restarts** box.

4. To change the time interval between attempts by the Job Manager to restart the job, select a number of minutes in the **Restart Interval (Mins)** box.

5. Click **OK** to save your changes.

CONFIGURE JOB RESTARTABILITY FOR AN INDIVIDUAL JOB

1. From the **Restore Options** dialog box, click **Advanced**, then select the **Job Retry** tab and specify the following as desired:
   - **Total Running Time** - The maximum elapsed time, in hours and minutes, from the time that the job is created.
   - **Number of Retries** - The number of times that Job Manager will attempt to restart the job.
   - **Kill Running Jobs When Total Running Time Expires** - Option to kill the job when the specified Total Running Time has elapsed, even if its state is "Running".

2. Click **OK.**

RESUBMIT JOBS

If a restore job fails to complete successfully, you can resubmit the job without the need to reconfigure the original job's restore options using the **Resubmit Job** feature. When a job is resubmitted, all the original options, restore destinations, and other settings configured for the job remain in tact.

RESUBMIT A RESTORE JOB

1. From the CommCell Browser, right-click a client computer whose data recovery history you want to view, click **View**, then click to view a job history.

2. From the **Job History Filter** dialog box, select **Restore.**
   - If you want to view more advanced options for restores, from the Job History Filter, select **Restore**, then click **Advanced**.
   - From the **Data Recovery History Advanced Filter** select the destination client computer of the restores you would like to view, then click **OK**.

3. The system displays the results of the options you selected in the **Data Recovery Job History** window.

4. Right-click on any job, and select **Resubmit**.

5. Select the job options.

6. Click **OK**.

CONTROL JOBS

The following controls are available for running jobs in the Job Controller window:

SUSPEND	Temporarily stops a job. A suspended job is not terminated; it can be restarted at a later time. Only preemptible jobs can be suspended.
RESUME	Resumes a job and returns the status to Waiting, Pending, Queued, or Running depending on the availability of resources or the state of the operation windows and activity control settings. Restore jobs for this Agent are resumed from the beginning.
KILL	Terminates a job.

These controls can be applied to:

- All jobs in the Job Controller.
- All selected jobs in the Job Controller providing you have the correct security associations at the proper level for each job selected.
- All data protection operations running for a particular client or client/agent.
- All data protection operations running for a particular MediaAgent.

CONTROL A JOB

1. From the Job Controller of the CommCell Console, right-click the job and select **Kill, Suspend,** or **Resume** as desired.
   - When killing a job:

     Click **Yes** when the confirmation prompt appears if you are sure you want to kill the job. The job status may change to **Kill Pending** for a few moments while the operation completes. Once completed, the job status will change to **Killed** and it will be removed from the Job Controller window after five minutes.
   - When suspending a job:

     The job status may change to **Suspend Pending** for a few moments while the operation completes. The job status then changes to **Suspended.**
   - When resuming a job:

     As the Job Manager attempts to restart the job, the job status changes to **Waiting**, **Pending**, or **Running**.

SETTING THE TIMEOUT VALUES FOR RECALL JOBS

Two registry keys are available for administering the timing of recalls. These keys work hand-in-hand with each other, and they are especially useful if the CommServe goes down:

- The nRETRY_RECALL_TIMEOUT registry key allows you to set the time of duration for a recall attempt. Once this time expires, the recall attempt will stop.

- The nRETRY_RECALL_DELAY key indicates the delay time for a recall attempt. Once this time expires, the recall attempt will resume.

ADDITIONAL RESTORE OPTIONS

Several additional options are available to further refine your restore operations. These options are available from the **Advanced Recover Options** window.

To access the **Advanced Recover Options** window:

1. From the CommCell Browser, expand **Client Computers** by double-clicking **Client Computers** | **File Archiver** | **<archive set name>**. The default and other subclients (if available) are displayed on the right-hand window pane.

2. To recover data from the archive set level, right-click the archive set, and click **Recover**.

3. From the **Unix File Archiver Recover Options** dialog box, click **Advanced**.

The additional options available in this dialog box are described below:

OPTION	DESCRIPTION	RELATED TOPIC
Startup Options	The Job Manager will use the startup priority setting when allocating the required resources. This is useful if you have jobs that are very important and must complete, or jobs that can be moved to a lower priority. 1. From the CommCell Browser, click **Client Computers**	**File Archiver**	**ArchiveSet**. The default and other subclients (if available) are displayed on the right-hand window pane. 2. From the CommCell Browser, right-click the archive set that contains the data you want to recover. Click **All Tasks** and then click **Browse**. 3. From the Browse Options window, click **OK**. 4. From the browse window, select the data to be restored and click **Recover all Selected.** 5. From the **Recover Options for All Selected Items** dialog box, click **Advanced**. 6. From the **Advanced Recover Options (Startup)** tab, select **Use Default Priority** option. 7. Select **Change Priority** option to change the priority for a job, between 0 (highest priority) and 999 (lowest priority). 8. Select **Start up in Suspended State** option to specify the selected job to start in the Job Controller in a suspended state. 9. Click **OK**.	Refer to Job Priority and Priority Precedence.
Copy Precedence	When you select Recover from copy precedence option, the system recovers data from the selected storage policy copy (Synchronous Copy or Selective Copy). If data does not exist in the specified copy, the data recovery or retrieve operation fails even if the data exists in another copy of the same storage policy. When cleared, (or by default) the system recovers or retrieves data from the storage policy copy with the lowest copy precedence. If the data was pruned from the primary copy, the system automatically recovers or retrieves from the other copies of the storage policy in the lowest copy precedence to highest copy precedence order. Once the data is found, it is recovered, and no further copies are checked. 1. From the CommCell Browser, click **Client Computers**	**File Archiver**	**ArchiveSet**. The default and other subclients (if available) are displayed on the right-hand window pane. 2. From the CommCell Browser, right-click the archive set that contains the data you want to recover. Click **All Tasks** and then click **Browse**. 3. From the Browse Options window, click **OK**. 4. From the browse window, select the data to be restored and click **Recover all Selected.** 5. From the **Recover Options for All Selected Items** dialog box, click **Advanced**. 6. From the **Advanced Recover Options (Copy Precedence)** tab, select **Recover from copy precedence** option. 7. Select the number to change the selected copy's precedence. The numbers will move a copy to a higher or lower precedence in increments of 1. 8. Click **OK**.	Refer to Recovering Data From Copies.
Data Path Options	Data Recovery operations use a specific data path (Library, MediaAgent, Drive Pool, and Drive) to perform the recover operations as configured in the CommCell. By default, the system automatically identifies the data path for the recover operations. You can change the data path at the restore level by selecting a specific MediaAgent, library, drive pool or drive in the Advanced Recover Options dialog. The following are some of the important situations where you may need to change the data path: - To free heavily loaded resources such as MediaAgents and libraries. - A library suffers severe hardware damage and you need to move its media to a different library in order to access data secured by data protection operations.	Refer to Change Data Path.

	● A drive pool within a library is being used much more frequently than another, and a storage policy copy from the more active drive pool can be assigned to the less active one. 1. From the CommCell Browser, click **Client Computers** | **File Archiver** | **ArchiveSet**. The default and other subclients (if available) are displayed on the right-hand window pane. 2. From the CommCell Browser, right-click the archive set that contains the data you want to recover. Click **All Tasks** and then click **Browse**. 3. From the Browse Options window, click **OK**. 4. From the browse window, select the data to be restored and click **Recover all Selected.** 5. From the **Recover Options for All Selected Items** dialog box, click **Advanced**. 6. From the **Advanced Recover Options (Data Path)** tab, select the **MediaAgent** and **Library** that you wish to perform the restore. 7. Select the **Drive Pool** and **Drive** for optical and tape libraries. 8. Click **OK**.	
Job Retry Options	The restore jobs can be restarted either by a user or automatically by the Job Manager. You can specify the maximum elapsed time before a job can be restarted or killed and the maximum number of restart attempts. 1. From the CommCell Browser, click **Client Computers** | **File Archiver** | **ArchiveSet**. The default and other subclients (if available) are displayed on the right-hand window pane. 2. From the CommCell Browser, right-click the archive set that contains the data you want to recover. Click **All Tasks** and then click **Browse**. 3. From the Browse Options window, click **OK**. 4. From the browse window, select the data to be restored and click **Recover all Selected.** 5. From the **Recover Options for All Selected Items** dialog box, click **Advanced**. 6. From the **Advanced Recover Options (Job Retry)** tab, select **Enable Total Running Time** option. 7. Select **Enable Number of Retries** option. 8. Select **Kill Running Jobs When Total Running Time Expires** option**.** 9. Click **OK**.	Refer to Job Management.
Restore Deleted Items	Deleted files can be manually restored by the user. You can specify the time range for the deleted items to be restored. 1. From the CommCell Browser, click **Client Computers** | **File Archiver** | **ArchiveSet**. The default and other subclients (if available) are displayed on the right-hand window pane. 2. From the CommCell Browser, right-click the archive set that contains the data you want to recover. Click **All Tasks** and then click **Browse**. 3. From the Browse Options window, click **OK**. 4. From the browse window, select the data to be restored and click **Recover all Selected.** 5. From the **Recover Options for All Selected Items** dialog box, click **Advanced**. 6. From the **Advanced Recover Options (Browse Options)** tab, select **Restore deleted items** option. 7. Select **Specify Time Range** option to specify the time zone, start time and end time for the deleted items to be restored. 8. Click **OK**.	
Alerts	The Alert option is used for setting up the criteria to raise notifications/alerts for job statuses such as failure, success, or any other conditions triggered by the restore job. Adding alerts helps the user or the user group to get the notification automatically about the status of the restore job. 1. From the CommCell Browser, click **Client Computers** | **File Archiver** | **ArchiveSet**. The default and other subclients (if available) are displayed on the right-hand window pane. 2. From the CommCell Browser, right-click the archive set that contains the data you want to recover. Click **All Tasks** and then click **Browse**. 3. From the Browse Options window, click **OK**. 4. From the browse window, select the data to be restored and click **Recover all Selected.** 5. From the **Recover Options for All Selected Items** dialog box, click **Advanced**. 6. From the **Advanced Recover Options (Alert)** tab, Click **Add Alert**. 7. From the Add Alert Wizard window, select the **Threshold and Notification Criteria**. Click **Next.** 8. Select the **Notification Types.** Click **Next.** 9. Select the **Users and User Groups.** Click **Next.**	Refer to Alert.

	10. Verify the **Summary**. 11. Click **Finish**.	

Modify Paths and/or Filters	During a recover operation, you can modify the folder where the items will be recovered from and filter the items you wish to exclude from the recover operation.
	
	1. From the CommCell Browser, click **Client Computers** | **File Archiver** | **ArchiveSet**. The default and other subclients (if available) are displayed on the right-hand window pane.
	
	2. From the CommCell Browser, right-click the archive set that contains the data you want to recover. Click **All Tasks** and then click **Browse**.
	
	3. From the Browse Options window, click **OK**.
	
	4. From the browse window, select the data to be restored and click **Recover all Selected.**
	
	5. From the **Recover Options for All Selected Items** dialog box, click **Advanced**.
	
	6. From the **Advanced Recover Options (Paths/Filters)** tab, do the following:
	   ○ For **Source Item**, click **Add** to enter a new file/folder to recover.
	   ○ For **Filter Item**, click **Add** to enter a file or subfolder to exclude during the recover operation.
	
	   You can also click **Delete** to remove existing source or filter items.	

Command Line Restores	Command Line Interface enables you to perform restore operations from the command line. The qcommands can be executed from the command line or can be integrated into your own scripts or scheduling programs. In addition, you can also generate scripts for specific operations from the CommCell Console using the Save As Script option. These scripts can later be executed using the commands from the command line interface.	Refer to Command Line Interface.
Restore Job Summary Report	Restore Job Summary Report provides you the summary of all restore jobs during a specified time period for each client. Select Restore option from the Job Summary Report Selection dialog box, to view the Restore Job Summary Report.	Refer to Restore Job Summary Report.

Data Aging - File Archiver

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**.
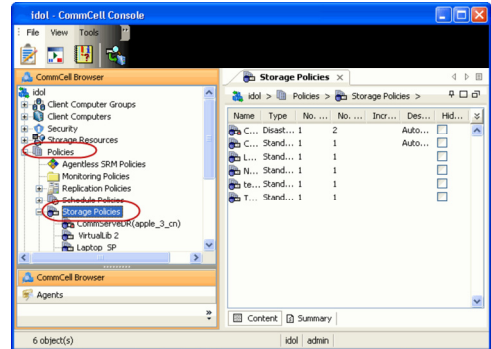
2. Highlight the **Storage Policy**.
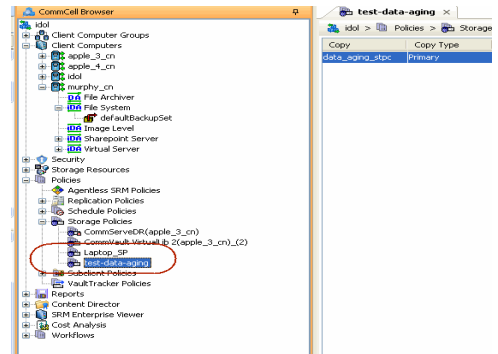
3. From the right pane, right-click the **Storage Policy Copy** and click the **Properties**.
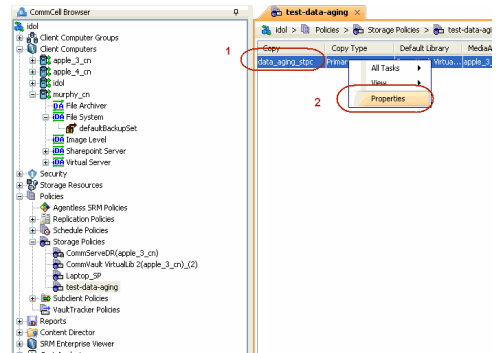
4.
   - Click the **Retention** tab.
   - Click the **Retain For** in the **Basic Retention Rules for All Backups** area.
   - Enter number of days to retain the data.
   - Enter number of cycles to retain the data.
   - Click **OK**.
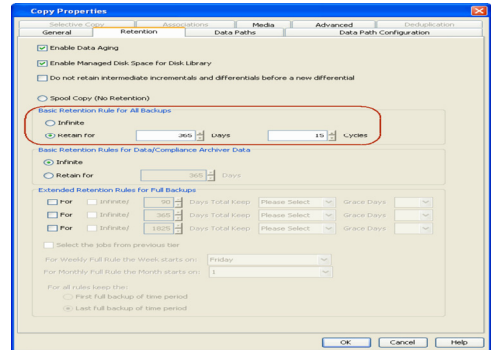
5. From the CommCell Browser, click the **Reports** icon.
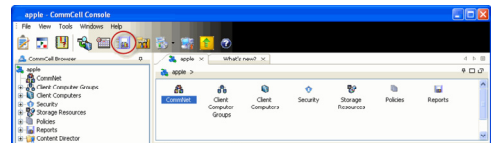
6. Expand Reports and select **Data Retention Forecast and Compliance.**
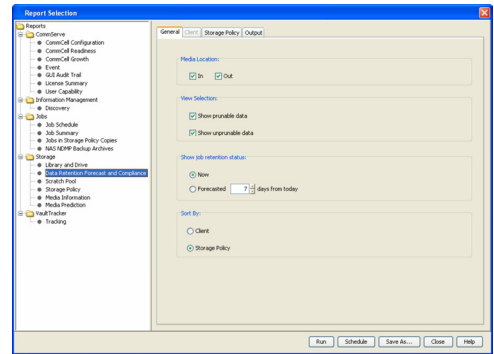
7. Click **Run**.
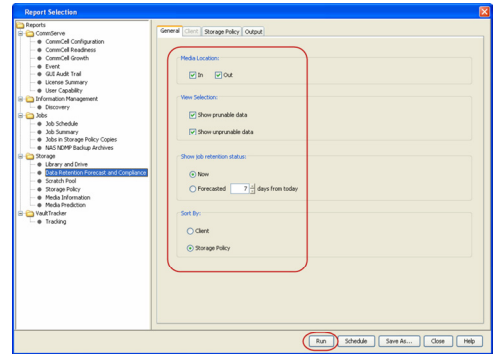
8. The report will display the data to be pruned when a data aging job is run.

> 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.
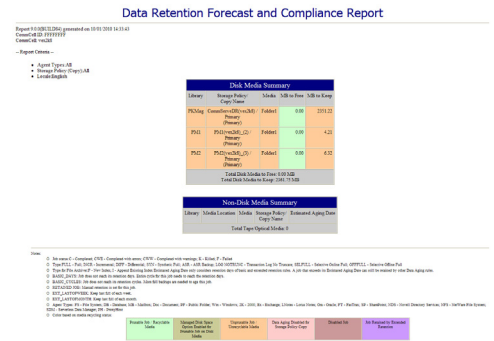
9. From the CommCell Console, right click the CommServe icon and click **All Tasks | Data Aging**.
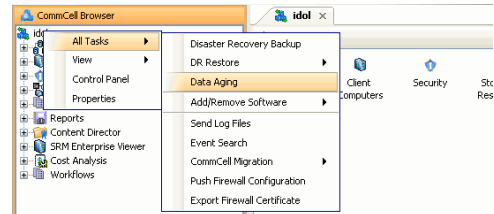
10. Select **Immediate** in the Job Initiation section and click **OK**.
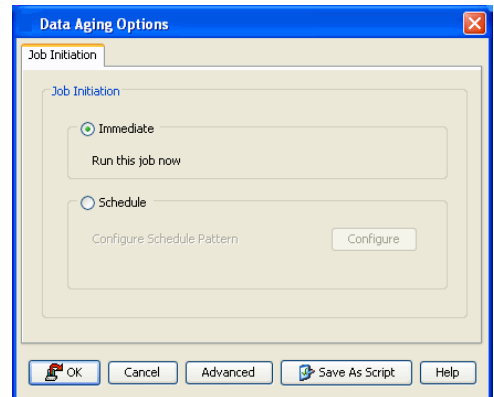
11. You can track the progress of the job from the **Job Controller** window. When the job has completed, the Job Controller displays **Completed**.
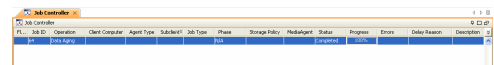
Make sure that the job completes successfully. If the job did not complete
successfully, re-run the job.

ADVANCED TOPICS

Data Aging - Advanced
Provides comprehensive information on additional Data Aging capabilities.

Additional Operations - File Archiver

RELATED TOPICS

Additional Operations - Concepts
Provides comprehensive information on additional operations procedures contained on this page.

● Audit Trail
● Storage Policies
● Storage Policy Copies
● Schedule Policy
● Auxiliary Copy
● Operation Window
● Uninstalling Components
● Global Filters

AUDIT TRAIL

The Audit Trail feature allows you to track the operations of users who have access to the CommCell. This capability is useful if a detrimental operation was performed in the CommCell and the source of that operation needs to be determined.

Audit Trail tracks operations according to four severity levels:

● **Critical**: This level records operations that will result in imminent loss of data.

● **High**: This level records operations that may result in loss of data.

● **Medium**: This level records changes to the general configuration of one or more entities. Such changes may produce unintended results when operations are performed.

● **Low**: This level records changes to status, addition of entities, and other operations that have minimal impact on existing CommCell functions.

To set Audit Trail retention periods:

1. From the **Tools** menu in the CommCell Console, click **Control Panel**, and then select **Audit Trail**.

2. From the **Audit Trail** dialog box, select the desired retention time (in days) for each severity level.

3. Click **OK**.

STORAGE POLICY

A Storage policy defines the data lifecycle management rules for protected data. Storage policies map data from its original location to a physical storage media and determine its retention period.

1. Expand the **Policies** node, right-click **Storage Policies**, and select **New Storage Policy**.

2. Click **Next.**

3. Select **Data Protection and Archiving** to create a regular storage policy or **CommServe Disaster Recovery Backup** to backup the CommServe database and click **Next**.

4. Click **Next**.

5. Enter the name of storage policy and click **Next**.

6. Enter the name of the primary copy and click **Next**.

7. From the drop down box, select the default library for the primary copy and click **Next**.

8. From the drop down box, select the MediaAgent and click **Next**.

9. Enter number of data streams and set the retention period for the policy and click **Next**.

10. Click **Next**.

11. Click **Browse,** browse to your designated deduplication store location and click **Next**.

12. Confirm your selections and click **Finish**.

SCHEDULE POLICY

A schedule policy is a defined schedule or group of schedules for specific operations to be performed on associated objects within the CommCell. When the schedules from a policy are run, the specified operations, (e.g., auxiliary copy, backup, etc.,) will be performed on the associated CommCell objects.

1. Expand the **Policies** node, right-click **Schedule Policies** and click **Add**.

2. Type the **Name** of the schedule policy.

3. Select the **Type** of schedule policy.

4. Select the **Agent Type**.

5. Type a description of the schedule policy.

6. Click **Add**.

7. Enter a Schedule Name in the **Schedule Pattern** tab.

8. Click **OK**.

9. On the **Associations** tab, select the objects to be associated with the schedule policy.

10. Click **OK**.

AUXILIARY COPY

An auxiliary copy operation allows you to create secondary copies of data associated with data protection operations, independent of the original copy.

1. Expand the **Policies** node, right-click storage policy for which you want to perform an auxiliary copy, click **All Tasks**, and then click **Run Auxiliary Copy**.

2. If you are starting the auxiliary copy operation from the CommServe level, select the storage policy for which you wish to perform the auxiliary copy.

> If you are starting the auxiliary copy operation from the Storage Policy level, 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. Click **OK** to start the auxiliary copy operation. A progress bar displays the progress of the operation.

OPERATION WINDOW

By default, all operations in the CommCell can run for 24 hours. To prevent certain operations from running during certain periods of the day, you can define operation rules so that these operations are disabled during those times.

When operation rules are configured, operations that are started within the time window specified will go to a queued (as opposed to pending) state. Once the time window specified in the operation rule has elapsed, these queued or running operations will resume automatically.

1. In the CommCell Browser, right-click the appropriate entity, click **All Tasks,** and then click **Operation Window**.

2. Click **Add**.

3. From the **Operation Window** dialog box:
   - Enter the name of the rule in the **Name** field.
   - Select either an administration, data protection (either full or non-full), and/or a data recovery operation from the **Operations** pane.

4. Click **OK**.

UNINSTALLING COMPONENTS

UNINSTALLING COMPONENTS FROM A UNIX CLIENT

UNINSTALL SEQUENCE

When uninstalling a component on a client computer, the following sequence must be used:

1. Uninstall all application components and updates.

2. Uninstall the MediaAgent (if one exists)

3. Uninstall the Base software

Since the component software depends upon the Base software, you must uninstall the component software first.

UNINSTALLING COMPONENTS FROM A UNIX CLUSTER

The following provide general guidelines for uninstalling components from a cluster.

- Clustered environments pertain only to HP-UX, Linux, and Solaris clients.
- Verify that the cluster is set to its original state (i.e., the active and passive nodes are in the same state of ownership for their disk groups as they were during installation).

- If the computer from which the component has been uninstalled is rebooted, services will not be restarted following the reboot. However, any cluster plug-ins available will continue to run.

- You will need to deconfigure the Unix File System *i*DataAgent from each virtual machine first before uninstalling it from the physical nodes.

- You will then need to uninstall the Unix File System *i*DataAgent and Base software (`cvpkgrm`) from the client computer hosting the software. You can uninstall the Base software from your client computer by entering the `cvpkgrm` command from a command line and then completing the directives in the resulting script. This script deletes the appropriate files and executables, and it removes the registry entries from the system.

- The component software allows you to Deconfigure virtual machines completely. It also allows you to Deconfigure individual modules for the virtual machines.

  To Deconfigure a virtual machine, the virtual machine must be Deconfigured from all of the physical machines (hosts) on which it has been configured. This means that, within a clustered environment, each virtual machine must be Deconfigured from at least two hosts. To do this, follow the sequence outlined in Components on Unix.

GLOBAL FILTERS

Global Filters are exclusions that can be set to filter out data from data protection operations. This is useful in cases where certain files, folders or entities need to be excluded from data protection operations.

Global Filters can be configured on either the CommNet or CommCell level. At the CommNet level, Global Filters exclude data from data protection operations on multiple CommCells at once. On the CommCell level, Global Filters exclude data from data protection operations on all clients residing within the CommCell.

ONLINE HELP LINKS

Use the following links to view the online help for the corresponding tabs in the CommCell Console:

OPERATIONS	ENTITY	ONLINE HELP LINKS
CONFIGURATION	Agent	Unix File Archiver Agent Properties (General)
		Unix File Archiver Agent Properties (Version)
		Unix File Archiver Agent Properties (Security)
		Unix File Archiver Agent Properties (Activity Control)
	Archive Set	Archive Set Properties (General)
		Archive Set Properties (Security)
	Subclient	Unix File Archiver Agent Subclient Properties (General)
		Unix File Archiver Agent Subclient Properties (Filters)
		Unix File Archiver Agent Subclient Properties (Pre/Post Process)
		Unix File Archiver Agent Subclient Properties (Security)
		Unix File Archiver Agent Subclient Properties (Encryption)
		Unix File Archiver Agent Subclient Properties (Storage Device)
		Unix File Archiver Agent Subclient Properties (Activity Control)
		Unix File Archiver Agent Subclient Properties (Content)
BROWSE		Unix File Archiver Browse Options
		Unix File Archiver Advanced Browse Options
		List Media
RESTORE	Restore Options	Restore Options by Jobs Filter
OPERATION WINDOW	Operation Window	Operation Window

Back to Top

Troubleshooting - File Archiver

The following section provides information on some of the troubleshooting scenarios related to file archiving:

ERROR MESSAGE DOES NOT APPEAR WHEN A RECALL JOB IS WAITING

SOLUTION

Set the number of mount retries. A failure notification will be displayed after the set number of mount retries. Use DMReadMaxMountRetryVal key for setting a finite number of mount retries during restore.

ARCHIVING IS FAILING DURING THE STUBBING PHASE

PROBLEM CAUSE

The archiving job is failing during the stubbing phase as the subclient content selected for the job is a nested mount point.

SOLUTION

For stubbing to work with nested mount points ensure that each mount point is individually selected as the subclient content for archiving.

ERROR OPENING TERMINAL SERVER <*HOSTNAME*>. ERROR [1722]:THE RPC SERVER IS UNAVAILABLE

ERROR OPENING TERMINAL SERVER <*HOSTNAME*>. ERROR [5]:ACCESS IS DENIED

PROBLEM

During recalls the File Archiver recall popup message is not being sent even though the Enable Recall Popup Message has been selected from the system tray settings of the notification enabler.

SOLUTION

- It is recommended to login with the domain account instead of the local administrator account. This allows for the GXHSMService to start with the domain account, which has the rights to send messages.
- If the recalls are being triggered from client computers, it is recommended to create the following Windows registry key in all the client computers:
  1. On the client computer, open the Registry Editor.
  2. In the left pane, navigate to **HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Terminal Server**.
  3. In the right pane, select the **AllowRemoteRPC** key and change its **Value** to **1**.
  4. Exit the Registry Editor and reboot the client computer.

MULTIPLE COPIES OF HARD LINKS ARE GETTING BACKED UP

PROBLEM CAUSE

Multiple copies of a hard link gets backed up because during the scan phase multiple copies of the hard link gets added to the collect file.

SOLUTION

To avoid backing up multiple copies of a hard link it is recommended to create the following registry key:

1. From the CommCell Browser, navigate to **Client Computers**.
2. Right-click the <*Client*> and then click **Properties**.
3. Click the **Registry Key Settings** tab.
4. Click **Add**.
5. In the **Name** field, type sHLINK.
6. In the **Location** list, type or select UnixFsDataMigrator.
7. In the **Type** list, select **Value**.
8. In the **Value** field, type **Y** to backup a single copy of the hardlinks.

9. Click **OK**.
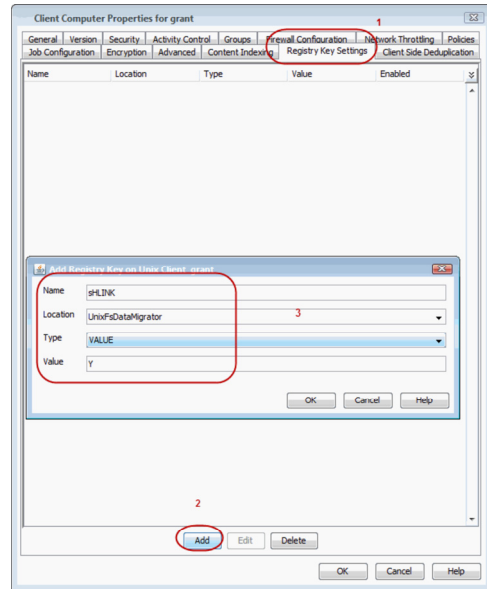
Online Help Topics

Agent Properties (General)

Use the Agent Properties (General) tab to obtain or provide general and/or user account information for the agent. Note that all the options described in this help may not be available and only the options displayed in the dialog box are applicable to the agent for which the information is being displayed.

Client (Computer, Name)

Displays the name of the client computer or application server.

Billing Department

Displays the name of the billing department, when the Agent is associated with a billing department. For more information on Billing and Costing See the *CommNet Books Online*.

***i*DataAgent/Agent (Type)**

Displays the identity of the agent that is installed on the client computer or application server.

Installed (date)

Displays the date on which the agent was installed or upgraded on the client computer or application server.

Auto Discover Instances

If selected during installation, this option will also be selected at the Agent level after the install is complete. When selected, instances are automatically discovered every 24 hours; or whenever the Communications Service (GxCVD) service is restarted. The default every 24 hours timing can be overridden with the nAutoDiscoverSQLInstanceTimeout registry key.

> For Express installations, an option does not appear during installation but instances are automatically discovered. By default, this option is automatically selected at the Agent level.

Manage Content Automatically

When selected, SQL databases that were automatically discovered but later deleted from an application (e.g., SQL Server) will be automatically deleted from the content of the default subclient when the next backup is run. This alleviates having to delete the databases manually. Databases that are manually added and later deleted from an application are not automatically removed from the subclient when the next backup runs and the backup job will complete with errors. By default, this is selected after client install or upgrade.

Enable Instance Discovery

When selected, instances are automatically discovered every 168 hours (one week) by default or whenever the Communications Service (GxCVD) service is restarted. The default 168 hour (one week) timing can be overridden with the nORACLEINSTANCEDISCOVERYINTERVAL registry key.

Stub Recovery Parameters

Specifies whether to enable recall throttling for stub recovery jobs. Selecting this option will allow you to control the number of stub recovery jobs that can be run based on the limits set below. When these options are disabled in the CommCell Console, the system will apply any legacy registry key settings corresponding to these options, where applicable.

> It is recommended not to recall more stubs than the limit specified under the Maximum Stub Recovery for Celerra Proxy as it does not detect failure and the data is lost.

- **Maximum Stub Recovery**

  Use this space to specify the upper limit for the number of stubs to be recovered for this agent.

- **Time between recall to count as successive in seconds**

  Use this space to specify the number of seconds for a recall to be considered as successive.

- **Time to wait after maximum successive recalls limit is reached in seconds**

  Use this space to specify the number of seconds that this agent must wait before additional stub recovery jobs can begin after the upper limit has been reached.

Erase Archive Data when Stub is Deleted

In the text box, specify the path where deleted stubs will be monitored for deletion when an Erase Data job is run. This could be the entire machine (indicated by a \), a particular drive (C:\), a particular folder (C:\deleted_data), or a UNC path (\\filer\directory). Multiple locations could also be specified, separated by the ; delimiter.

- The path that is configured here will be applicable for all instances of the File Archiver for Windows Agent.
- For **Local File System** instances, a folder can be created to contain the stubs to be hard-deleted (SHIFT_DELETE).

> This folder would then be part of the path that is specified (e.g., `(C:\deleted_data)`. This would alleviate specifying entire volumes. From the volumes, you can then move the stubs (cut+paste) to the specified deletion folder. To move stubs across volumes, you must use the GxhsmUtility tool in the Resource Pack.
>
> - For **Celerra** and **FPolicy** instances, a folder cannot be created to contain the stubs to be deleted. You can instead restrict the deletion to certain folders by specifying a subclient path or a path that is a parent to the subclient path.
> - The path that is configured here is only used when an Erase Data job is run.
> - If you delete stubs within the path that is specified and the subclient that includes the path is deleted, the data will not be erased.
> - For **FPolicy** instances, the user must either specify "\" or a specific deletion folder path. If the intended deletion folder path is `\\<filer_name>\<volume_name>\<folder_name>`, the deletion folder specification needs to be:
>
>   `\\<fully_qualified_filer_name>\ONTAP_ADMIN$\vol\<volume_name>\<folder_name>;\\<short_filer_name>\ONTAP_ADMIN$\vol\<volume_name>\<folder_name>`. Otherwise, the data will not be erased.
>
> - For local data archived by a **Local File System** instance, the stubs must be permanently deleted with a hard-delete (SHIFT+DELETE). Stubs that are removed with a soft-delete (DELETE or right-click and DELETE) will not be erased.

NDS Tree Name

Displays the name of the NDS tree that this agent can access.

NDMP Properties

Click to access the **NDMP Server Properties** screen.

NDMP Restore Enabled

Specifies whether the NDMP Restore Enabler was installed with the *i*DataAgent.

- **YES** indicates that the enabler is installed and the client is an available destination for the restore of data from a Network Attached Storage (NAS) client.
- **NO** indicates that the enabler is not installed and the client is not an available destination for the restore of data from a NAS client.

QSnap Maximum Cache Size (in MB)

Specifies the maximum cache size for QSnap. See **Books Online** for more information on QSnap, before changing the maximum cache size.

QSnap Minimum Cache Size (in MB)

Specifies the minimum cache size for QSnap. See the **Books Online** for more information on QSnap, before changing the minimum cache size.

User Account

Displays the user account used by the system to log in to or access the (the tree of the) server during various jobs (including backups, browses, restores, etc.). For NAS NDMP, displays the NDMP account used by the system to connect to the NAS data server.

Administrative Group Account

Displays the SharePoint Administrator Account that has required rights to create and modify SharePoint databases. This account will be used for data protection and recovery operations.

SSO Account

Displays the SSO Administrator account for the single sign-on service on this SharePoint Server.

Change Account

Click to specify a different account as the **User Account**.

SharePoint Server Name

Displays the name of the SharePoint Server that is installed on the client computer. You can use this space to modify this server name if the name displayed is incorrect (e.g., not the same as the Client name or Host name).

Index Backup/Restore path

The UNC path for a shared network folder to temporarily store the site index during backup and restore. There should be enough space available on the share for the index to be temporarily stored.

> For a SharePoint All-in-One Server, the Index path must be local, not a UNC path.

If topology manager is locked during backup/restore, force its release

Specifies whether the system should release the lock for the topology manager and therefore allow jobs to complete without interruption. This option is selected by default for new installations.

SQL Databases hosted on a remote SQL Server

Specifies whether the SharePoint Server is part of a SharePoint Server Farm and whether the SQL Databases are hosted on a remote SQL Server. If selected, the SQL Databases must be backed up using the SQL Server *i*DataAgent.

Authenticate Active Directory Domain Controller

Specifies whether to use or change the user account to authenticate against the Active Directory domain controller to look up group membership for the specified user (per the following fields)

Domain Name

Use this space to enter the domain name for this user.

User Name

Use this space to enter the name of the user for the account discussed for the preceding field.

For CDR, displays the user account to be used for the creation of ONTAP snapshots.

Password

Use this space to enter the password for this user.

Confirm Password

Retype the password.

Description

Use this field to enter a description about the entity. This description can include information about the entity's content, cautionary notes, etc.

Enable Offline Mining

Select this option to enable browse and restore of offline data.

Enable Office Communication Server Backup

Select this option to enable OCS backup feature for a client with Windows File System _i_DataAgent. This feature provides the ability to perform data protection operations for data associated with the Office Communications Server.

Enable SRM feature

Select this option to Enable SRM Options.

Enable for Archiving

Select this option to enable archiving for the agent. Once selected a license will be consumed.

Back to Top

Version

Use this dialog box to view the software version and verify the update status. Note that all the options described in this help may not be available and only the options displayed in the dialog box are applicable to the agent for which the information is being displayed.

Software Install Directory

Displays the directory path in which the software is currently installed on the client or MediaAgent computer.

Crypto Library Version

Displays the current version of the Crypto Library module.

Version Information

Displays the software component version (CommServe, MediaAgent, Client or Agent) installed on the computer.

Update Status

Displays the update status for each client computer. The possible values and their descriptions are:

- **Unknown**

  The software is not able to determine if the client computer meets the baseline level of updates due to an error or an uninstalled client still showing in the CommCell console.

- **Has Diagnostic**

  One or more diagnostic updates have been installed on the client computer.

- **Up To Date**

  The updates in the client computer match the baseline.

- **Needs Update**

The client computer must be updated to meet the baseline level of updates.

● **Ahead of Cache**

The client computer exceeds the baseline level of updates in the CommServe Cache directory.

Package

Displays the name of the packages installed on the client.

Status

Displays the update status for each package. The possible values are: *Unknown*, *Has Diagnostic, Up To Date*, *Needs Update*, and *Ahead of Cache*. (Refer to previous section for a description of these values.)

Updates

Displays the name of the updates.

Update Information

Specifies the options for installing the updates.

This information is displayed only in the case of remote clients and/or remote MediaAgents. (A client/MediaAgent that is not installed on the CommServe computer)

● **Cache Source**

This information is only displayed for client computers.

○ **CommServe**

If selected, the selected client receives its updates from the CommServe computer.

○ **Software Cache**

If selected, the selected client receives its updates from the specified Client designated as Software Cache computer.

● **Store Updates Locally**

When selected, indicates that the update packages must be saved on the local computer, before they are installed. Use the space to type the location on the local computer in which the updates must be stored, or click the **Browse** button to select the location on the local computer.

If this option is selected, make sure that there is adequate space for installing the necessary updates. Also note that the system automatically deletes the update packages once they are installed.
(You cannot specify a different folder to serve as the temporary cache location for NetWare clients; this field is disabled.)

Security

Use this dialog box to:

● Identify the user groups to which this CommCell object is associated.

● Associate this object with a user group.

● Disassociate this object from a user group.

Available Groups

Displays the names of the user groups that are not associated with this CommCell object.

Associated Groups

Displays the names of user groups that are associated with this CommCell object.

Automatically add New Users to the "View All" Group (CommServe Level Only)

Specifies that all new users will automatically be added to the View All user group. This group allows users to view all CommCell objects, regardless of the associations of the other user groups they belong to.

Require Authentication for Agent Installation (CommServe Level Only)

Enable this option to prompt users for authentication for any agent installation on the CommCell.

Client Owners

Specify a user to allow CommCell user access to this client computer through CommCell Console and allow permission to run Web Console browse and restore operations on this client. Each user must be listed in a separate line.

Activity Control

Use this dialog box to enable or disable data management and data recovery on a selected client computer group, client computer, agent, or subclient. Note that not all agents support subclients. For the File Archiver for Windows Agent, use this dialog box to enable or disable Data Classification. Also note that all the options described in this help may not be available and only the options displayed in the dialog box are applicable to the agent for which the information is being displayed.

If data management and data recovery operations are disabled at the client computer group or client level, then these operations below these levels will be disabled. If data management / data recovery operations are enabled at the client computer group or client level, then these operations below these levels will be enabled.

Enable Data Management / Backups / Archive / QR Volume Creation

Specifies whether data management operations (Backups / Archive / QR Volume Creation) will occur from this client computer group, client computer, agent or subclient.

If cleared:

- The button **Enable after a Delay** appears to the right side of this operation activity. It allows to pre-determine the date and time at which data management operations will begin on the selected client computer group, client computer, agent, or subclient.
- Data management operations from this client computer group, client computer, agent, or subclient cannot be started and are skipped.
- Running and waiting data management operations for this client computer group, client computer, agent, or subclient run to completion.
- Stopped data management operations for this client computer group, client computer, agent, or subclient cannot be resumed until this option is enabled.
- Pending data management operations for this client computer group, client computer, agent, or subclient do not run until this option is enabled.

(Job states are indicated in the Job Controller.)

Enable Data Recovery / Restores / Retrieve / QR Volume Recovery (Not applicable for the subclient level)

Specifies whether data recovery operations (Restores / Retrieve / QR Volume Recovery) will occur from this client computer group, client computer or agent.

If cleared:

- The button **Enable after a Delay** appears to the right side of this operation activity. It allows to pre-determine the date and time at which data recovery operations will begin on the selected client computer group, client computer, or agent.
- Data recovery operations for this client computer group, client computer or agent cannot be started and are skipped.
- Running data recovery operations for this client computer group, client computer or agent run to completion.
- Pending data recovery operations for this client computer group, client computer or agent do not run until data recovery operations are enabled.

(Job states are indicated in the Job Controller.)

Enable Content Indexing

Specifies whether Content Indexing operations will occur from this client computer group, client computer or agent.

If cleared:

- The button **Enable after a Delay** appears to the right side of this operation activity. It allows to pre-determine the date and time at which Content Indexing operations will begin on the selected client computer group, client computer, or agent.
- Content Indexing operations are not started and are skipped.
- Running and waiting Content Indexing operations run to completion.
- Content Indexing operations in a pending, queued, or suspended state cannot be resumed until this option is enabled.
- Pending Content Indexing operations cannot run until this option is enabled.

(Job states are indicated by the Job Controller.)

Enable SRM Data Collection

Specifies whether data collection operations will occur from this agent.

If cleared:

- The button **Enable after a Delay** appears to the right side of this operation activity. It allows to pre-determine the date and time at which data collection operations will begin on the selected agent.
- Data Collection operations are not started and are skipped.
- Running and waiting Data Collection operations run to completion.
- Data Collection operations in a pending, queued, or suspended state cannot be resumed until this option is enabled.
- Pending Data Collection operations cannot run until this option is enabled.

(Job states are indicated in the Job Controller.)

Enable Discovery

Specifies whether discovery operations will occur.

Script Preview

Click to display the backup script, based on the current subclient configuration, that will be submitted to RMAN when backups are performed for the selected Oracle subclient.

Backup Set / Archive Set Properties (General)

- Use the **Backup Set / Archive Set (General)** tab to change the configuration of the selected backup set / archive set.
- Use the **New Backup Set / New Archive Set** dialog box to define a new backup set.
- Use the **On Demand Backup Set / Archive Set (General)** tab to change the configuration of the selected backup set / archive set.
- Use the **Create New On Demand Backup Set / Archive Set** dialog box to define a new on demand backup set / archive set.

Note that all the options described in this help may not be available and only the options displayed in the dialog box are applicable to the agent for which the information is being displayed.

Client Name / Client Computer

Displays the name of the Client computer on which this backup set / archive set is found.

Billing Department

Displays the name of the billing department, when the backup set is associated with a billing department. For more information on Billing and Costing See the *CommNet Books Online*.

Agent Type / _i_DataAgent

Displays the name of the _i_DataAgent to which this backup set / archive set belongs.

Instance

Displays the name of the instance to which this backup set belongs.

Partition

Displays the Lotus Domino Server data path under which this data is found.

Database Name

Displays the name of the database.

Replication Set

The name of the Replication Set for which the system automatically created this backup set and its default subclient.

Backup Set / New Backup Set Name

Specifies the name of the Backup Set. You can use this space to create or modify a name. (Backup Sets for certain _i_DataAgents cannot be modified.)

Choose Backupset Type

- **SharePoint Server Document**

  The content of this backup set can specify backing up site collections, sub-sites, areas, libraries, and lists.

- **SharePoint Server Database**

  The content of this backup set specifies backing up SharePoint 2007 site collections, WSS web application content databases, shared service providers, WSS searches, global search settings.

- **Force use of V2 APIs**

  Specifies to backup SharePoint 2003 site collections, portal sites, site content databases, site indexes, teamsite databases, and webstorage system databases.

Image Backup Set

Specifies whether the selected backup set will perform a SnapMirror to Tape (aka smtape) block backup. These backup types are supported for NetApp file servers running ONTAP 8.0 or higher. These types of backups are useful if the volumes on the filers contain mirrored snapshots. Moving mirrored snapshots to tape saves filer disk space and provides fast point-in-time volume recovery of mirrored data.

Type

Displays the SharePoint Server version. Applicable only on machines where both SharePoint Server 2003 and 2007 versions exist.

Archive Set / New Archive Set Name

Displays the name of the archive set. If applicable, use this space to enter or change the name of the archive set.

On Demand

Displays whether the selected backup set / archive set is an On Demand Backup Set / Archive Set.

Make this the Default backup set

Specifies whether the selected backup set is the default or a user-defined backup. Selecting this option asserts this backup set as the default. The previously designated default backup set is automatically reallocated as a user-defined backup set. Clearing this option, is accomplished by opening the Backup Set Properties dialog box of some other backup set and clicking this option there, thereby designating that backup set as the default.

Subclient Content may contain Wildcard Entries

Allows for the selection of files with specified extensions that can be backed up during the backup operation.

Make this the Default archive set

Displays whether the selected archive set is the default, in cases where other types of archive sets are also supported on the same agent (for example: User-Defined Archive Set, DataClassSet, On Demand Archive Set).

Subclient Policy

Displays the name of the Subclient Policy associated with this backup set. If no Subclient Policy is associated with this backup set, it will display "<None>".

Job Options

● **Use Change Journal**

Specifies that NTFS change journal is used to determine whether files have been modified for all subclients within the backup set.

● **Use Classic File Scan**

Specifies that the classic file scan is used to determine whether files have been modified for all subclients within the backup set.

Preserve File Access Time

Specifies whether the file access time is preserved and therefore not modified at the time of backup. Selecting this option may increase the time required to complete a backup.

Check Archive Bit During Backups

Specifies whether files are considered modified and therefore backed up based on either the state of the archive bit or the file modification time. In addition, the system resets the Archive bit of every file that it backs up. This option influences the way incremental and differential backups are conducted for all subclients within the backup set. It does not affect the behavior of full backups.

● **Use Data Classification**

Specifies that the Data Classification Enabler is used to determine whether files have been modified for all subclients within the backup set.

	This field is disabled for Online Content Indexing for NAS File Servers.

● **Decompress Data before Backup**

Specifies that data on a compressed drive is decompressed before being sent to the backup media, thereby preventing data recovery failures when restoring data to a volume that does not support compression. By default, data is backed up in compressed format if the data is on a volume that supports compression. When this option is initially selected, the next backup for each subclient within the backup set is converted to a full. This ensures that all of the client's compressed data is decompressed, including all data backed up prior to this selection.

Next Backup

Displays whether the next backup job may be full or non-full. When Next Backup displays Full the next backup job will be changed to a full.

Available DB Names

Select the database name(s) to be used as backup set name(s) by clicking the database name(s) and then clicking > to move the name(s) into `Selection`.

Selection

Specify the appropriate backup set (database) name(s) from the Available `DB Names`.

Storage Policy for All Log Files

Specifies the storage policy for all the log files in this backup set. You can use the list to change the storage policy.

Catalog Partition No.

Specifies the number of the catalog partition database for the DB2 DPF instance. This is the partition through which access to all system tables must go.

Connect as a Different User

Specifies to connect to the DB2 application using a different DB2 user account.

User Account

Displays the application User account used by the system to perform all Data Protection and Recovery operations for this backup set.

Change

Click to change the application user account.

Status of <database>

Displays the status of the database (backup set) as either CONNECTED or DISCONNECTED.

Refresh

Displays the most current status of the database.

Subclient

Displays those subclients that belong to the backup set / archive set.

Storage Policies

Select a storage policy from the list.

Enable Auto-Discover

Specifies whether to enable auto-discovery of new databases for all subclients of this backup set. Selecting this option will cause the system to discover and assign any new databases at the beginning of each backup operation. This option is available only for default dump backup set of postgresql *i*DataAgents.

Description

Use this field to enter a description about the entity. This description can include information about the entity's content, cautionary notes, etc.

Add

Click to create a subclient for the backup set / archive set.

Edit

Click to change the properties of a subclient that you select from the list.

Delete

Removes a subclient that you select from the list.

Back to Top

Subclient Properties (General)

Use Subclient Properties (General) tab to add, modify or view general information on the selected subclient. Note that all the options described in this help may not be available and only the options displayed in the dialog box are applicable to the agent or enabler for which the information is being displayed.

Client Computer / Client Name

Displays the name of the Client computer to which this subclient belongs.

Billable Entity

The name of the Billable Entity assigned to this subclient.

Billing Department

Displays the name of the billing department, when the subclient is associated with a billing department. For more information on Billing and Costing See the *CommNet Books Online*.

***i*DataAgent/Agent Type**

Displays the name of the Agent to which this subclient belongs.

Backup Set

Displays the name of the Backup Set to which this subclient belongs.

Instance

Displays the name of the Instance to which this subclient belongs.

Policy (External Data Connector Only)

Displays the name of this policy. You can use this space to enter or modify the name of the policy.

Database Name

Displays the name of the Database to which this subclient belongs.

Partition

Displays the Lotus Domino Server data path under which data is found for this subclient.

Subclient Name

Displays the name of this Subclient. You can use this space to enter or modify the name of the subclient.

Policy Name

Displays the name of this policy. You can use this space to enter or modify the name of the policy.

Subclient Type

Displays whether this subclient is a database or file/file group type.

Incremental Support Using

- **CXBF**

  Select this option to perform a CXBF backup for the selected subclient.

- **Checksum**

  Select this option to perform a non-CXBF (Checksum) backup for the selected subclient.

Discover Criteria (External Data Connector Only)

- **All**

  This option discovers all clients associated with the master server.

- **By Agent Type**

  This option discovers clients containing the Agent selected in the drop-down menu.

- **By Client Names**

  This option discovers clients by their names.

- **Select Client Group for Discovered Clients**

  Select a Client group to associate discovered clients to. If desired, you can also **Create a New Group**.

Disable Auto-Discovery

Specified to disable the auto-discovery and pre-assignment of SQL databases to the default subclient. By default, SQL databases are automatically discovered and assigned to the default subclient.

Create New Index Every *nn* Archive Operations

Displays the interval for index creation by number of archive operations on this subclient. You can use this space to modify the interval setting. This setting can be overridden by selecting the Create New Index option on the Advanced Backup/Archive Options (Data) tab. If overridden, the new index interval counter will start again at zero.

Set index cycle to every *nn* backup jobs

For the default subclient of an On Demand Backup Set, displays the interval for index creation by number of backup or migration operations on this subclient. You can use this space to modify the interval setting. This setting can be overridden by selecting the Create New Index option on the Advanced Backup/Migration Options (Data) tab.

Use Direct Database Access

Specifies to use the alternate read-only direct access to the SharePoint database to backup objects (e.g., documents, list items) and their metadata. This method can increase the backup speed and is applicable for Document backup sets, WSS v3.0, and MOSS 2007 environments. Requires installing specifically Microsoft SQL Server Native Client 2005 on Front-End Web Server. When selected or deselected, the next backup that is run will be a Full backup.

Use Direct Access to Restore Selected Entities

Specifies to restore individual files into the database directly. This is applicable for files in Document backup sets. When restoring the files directly into the database, the IDs of the files will remain the same and will not change.

Use content file provided by SRM

Uses content file consisting of files and directories provided by SRM report with on demand action.

Use VSS

Specifies whether VSS will be used to back up data for this subclient.

Use VSS for System State

Specifies whether VSS will be used to back up the system state for this subclient.

Use QSnap to handle backup of locked files

Specifies whether QSnap will be used to back up data (locked files) for this subclient.

Number of Data Readers

Use this space to specify the number of simultaneous backup data streams allowed for this subclient. For best performance, this should be set no higher than the number of physical drives that hold this subclient's data, except for specialized hardware such as RAID. For more information, see *Automatic File System Multi-Streaming* or *Backup - NAS NDMP* in Books Online.

Allow multiple data readers within a drive or mount point

Specifies whether multiple data reads are allowed for a single Windows physical drive or Unix mount point during backups on this subclient. This should be selected only for specialized hardware such as RAID, or possibly in the case of spanned volumes. For more information, see *Automatic File System Multi-Streaming* in Books Online.

Incremental backup should use

- **UNIX mtime**

  Select this option to determine which files are selected for incremental backup by changes in the mtime timestamp.

- **UNIX ctime**

  Select this option to determine which files are selected for incremental backup by changes in the ctime timestamp.

  When you select **Use Data Classification** in Backup Set Properties, it is recommended not to select "UNIX mtime" and "UNIX ctime" options in this properties box as Incremental Backups for Data Classification scan does not support these options.

Informix Server

Displays the name of the Informix instance to which this subclient belongs.

Default Subclient

Displays whether this is the default subclient. When a subclient is designated as the default subclient, it will back up/archive all the data for the subclient that is not assigned to any other subclients within the backup set/archive, and it cannot be deleted.

Offline Archive

Specifies whether to enable Offline Archive operations on this subclient to allow Outlook Add-In users the capability of retaining a full copy of archived items in local cache on the Outlook client.

Celerra Proxy Stub Subclient

Use the following group of options to enter or change the configuration information for the Proxy Stub Subclient feature.

- **Proxy Stub Path**

  Use this space to enter, or **Browse** to, the location of the directory on the server where the stubs will reside.

- **HTTP/CIFS Address**

  Use this space to enter the HTTP/CIFS address of the proxy stub path specified in the connection configured between the filer and the server.

- **NAS HTTP Port No.**

  Displays the port number used for communication with the proxy computer.

Collect User Identity

Specifies that during an archive operation, additional ownership/user information is collected and archived . This information is later used to perform owner based searches.

Operate in Archive Mode (Domino Mailbox Archiver Agent)

When selected, the Domino Mailbox Archiver Agent will perform archive operations based on the rules established in the **Archive Rules** tab of the **Subclient Properties** dialog box.

- **Operate in Backfill Mode** (Domino Mailbox Archiver Agent)

  When selected, this mode allows you to backup and populate the content index with messages that were sent and/or delivered before the point-in-time at which archives of the journaling mailbox begin.

Operate in Backup Mode Domino Mailbox Archiver Agent)

When selected, this mode allows you to perform full, incremental, differential, or synthetic full backups of mailbox databases using the Domino Mailbox Archiver

Agent. The **Archive Rules** tab of the **Subclient Properties** dialog box is disabled, backup operations run with no stubbing phase, and all mailbox data (with the exception of design documents) is backed in a similar fashion to the Lotus Notes Document *i*DataAgent.

Description

Use this field to enter a description about the entity. This description can include information about the entity's content, cautionary notes, etc.

Filters

Use this tab to add, modify or view the data protection or discovery filter on the selected subclient or Replication Set. Note that all the options described in this help may not be available and only the options displayed in the dialog box are applicable to the agent for which the information is being displayed.

Include Policy Filters

Specifies whether Subclient Policy filters will be used for this subclient, and is applicable only for subclients associated to a Subclient Policy. Selecting this option will cause this subclient to inherit the filter specified in the associated Subclient Policy. Clearing this option overrides the use of Subclient Policy filters on this subclient. See Subclient Policy - Filtering Rules for more information.

Include CommCell Level Global Filters / Global Filter

Specifies whether filters set under Control Panel (Global Filters) will be used in addition to the filters set at the subclient level to exclude data from data protection operations for this subclient.

Include Global Filters

Displays a list of options for enabling or disabling Global Filters which can be used in addition to the filters set at the subclient level to exclude data from data protection operations for this subclient. To change the setting, select one of the following values from the list:

- **OFF** - Disables Global Filters for this subclient.
- **ON** - Enables Global Filters for this subclient.
- **Use Cell Level Policy** - Enables or disables Global Filters for this subclient depending on whether the **Use Global Filters on All Subclients** option is enabled or disabled on the Control Panel (Global Filters) dialog. If the **Use Global Filters on All Subclients** option is enabled, then the **Use Cell Level Policy** option will enable Global Filters on this subclient. If the **Use Global Filters on All Subclients** option is disabled, then the **Use Cell Level Policy** option will disable Global Filters on this subclient.

Exclude these files/folders/directories/patterns/containers/objects

Displays entries that will be excluded from data protection operations for this subclient or Replication Set.

Regular Expressions

Provided below are details regarding support for the use of regular expressions (or wildcard characters) when adding entries to this exclusion list:

- Exchange Public Folder, Exchange Public Folder Archiver, Novell Directory Services (NDS), and SharePoint Document do not support the use of wildcards when adding entries to this set of exclusions.
- File Share Archiver - If a disk mount path is pointing to a filer share that will be archived, do not include UNC paths in the subclient content. UNC paths cannot be manually filtered out.
- For NAS NDMP *i*DataAgents:
  - BlueArc NAS NDMP - has no limitations. The * wild card is supported at the end of a directory filter (filters starting with /) or at the beginning or end of a file filter (not starting with /).
  - EMC Celerra NAS NDMP:
    - For older versions of DART OS (prior to 5.5), backup filters are not supported. Overlapping content cannot be configured. You cannot have one subclient with /myfs and another with /myfs/dir3. For example, if the default subclient specifies / as the content, and another subclient has /myfs/dir3 defined in the content, then backing up the default subclient will skip all of /myfs.
    - For DART OS 5.5 and above, filters are supported but do not work with volume-based backups. They are not blocked from being specified as an Advanced Backup/Archive Option , but a warning is displayed that the filters are ignored.
    - For DART OS 5.5 and above, a maximum of six directory filters (filters starting with /) and six file filters can be specified in either the default or user-defined subclients. If more filters are specified, a warning is displayed in the Event Viewer. For example, if a subclient specifies /myfs as the content, and another subclient specifies a total of 12 paths (/myfs/dir1 through /myfs/dir12), then when backing up the first subclient, you will receive six warnings indicating /myfs/dir7 through /myfs/dir12) were not filtered.
      - For directory filters, the * wild card is supported only at the end of the filter.
      - For file filters (not starting with /) the ? wild card matches a single character and the * wild card matches a string of characters. One of these wild cards can be used at the beginning or at the end of the filter.
  - Hitachi NAS NDMP - backup filters are not supported.
  - NetApp NAS NDMP:

- Backup filters can be used for file or folder names, but not paths. Thus, if the same filtered file name exists in multiple folders, all occurrences will be filtered. See *Subclients - NAS NDMP* in *Books Online* for details.
    - A maximum of 32 filters can be specified. The * wild card is supported, but only as the first or last character in the filter.
    - Filters are not supported for the GX model.
- For the Windows, NetWare, Unix, File Archiver Agents, and ContinuousDataReplicator Agents, see Wildcards for more information.

System State Filters

Following is a list of acceptable exclusion filters for Windows File System System State:

- {System Protected Files}
- {IIS}
- {COM+ Database}
- {Event Logs}
- {One Touch Files}
- {RSM}
- {Terminal Services Licensing}
- {Disk Quotas}
- {Content Indexing Catalogs}
- {WMI Database}
- {DHCP}
- {WINS}
- {UDDI Database}
- {Remote Storage Database}
- {Certificate Services }
- {Offline Files}
- {Active Directory Application Mode}
- {File Server Resource Manager}
- {NPS Database}

Exclude the following mailboxes/folders

Displays mailboxes or folders that will be excluded from data protection operations for this subclient. Wildcards are not supported when adding entries to this exclusion list.

Exclude the folders that contain the following patterns

Displays mailbox folder name wildcard patterns that will be excluded from data protection operations for this subclient. The Exchange Mailbox Archiver Agent, and the Exchange Compliance Archiver Agent support the use of wildcard expressions when adding entries to this exclusion list. See Wildcards for more information.

The following paths and files are excluded

Displays entries that will be excluded from discovery operations for this subclient. The Lotus Notes Database, Domino Mailbox Archiver, and Lotus Notes Document *i*DataAgents support the use of wildcard expressions when adding entries to this exclusion list. See Wildcards for more information.

Pattern/path to be excluded

Use this space to enter the path of a folder or file that you want to exclude from discovery operations for this subclient. The path must start with a (\), and it must be relative to the data path of the partition. The Lotus Notes Database, Domino Mailbox Archiver, and Lotus Notes Document *i*DataAgents support the use of wildcard expressions when adding entries to this exclusion list. See Wildcards for more information.

Except for these files/folders/directories/containers/objects

Displays entries that will be included in data protection operations for this subclient or Replication Set in cases where a parent object is listed in the Exclude filter.

Provided below are details regarding adding entries to this exceptions list:

- Wildcards are not supported in Exception filters.
- For NAS NDMP *i*DataAgents, only file names or folder names are valid entries when adding entries to this set of exceptions; paths are not supported.

Include these files/folders/patterns with every archive

Displays entries that will be included in archive operations for this subclient in cases where a parent object is listed in the Exclude filter. Note that File Archiver Agents do not support the use of regular expressions (or wildcard characters) when adding entries to this inclusions list.

- File Share Archiver - If a disk mount path is pointing to a filer share that will be archived, do not include UNC paths in the subclient content. UNC paths

cannot be manually filtered out.

Add

Click to manually add an entry to be included in, or excluded from, data protection operations for this subclient or Replication Set.

Browse

Click to browse for an entry to be included in, or excluded from, data protection operations for this subclient or Replication Set.

Edit

Click to manually edit an entry to be included in, or excluded from, data protection operations for this subclient.

Delete

Click to delete a selected filter entry.

Back to Top

Pre/Post Process

Use the Pre/Post Process tab to add, modify or view Pre/Post processes for the selected subclient or Replication Set. Note that all the options described in this help may not be available and only the options displayed in the dialog box are applicable to the agent or enabler for which the information is being displayed.

Pre Backup/Scan/Migrate/Archive/Copy/Snap/Recovery Point process

Displays the name/path of the process that you want to run before the respective phase. You can use this space to enter a process that will execute before this phase on the subclient or Replication Set, or you can use the **Browse** button to search for and select the name/path of the process. The system allows the use of spaces in the name/path, provided they begin with an opening quotation mark and end with a closing quotation mark.

	If you are using the Linux File System *i*DataAgent to back up VMware virtual machines, you must create a PreBackup process script that will allow the system to create the required REDO files. See "Create Pre/Post Backup Process Scripts to Back up VMware Virtual Machines Using the Linux File System *i*DataAgent" in Books Online for step-by-step instructions.

Post Backup/Scan/Migrate/Archive/Copy/Snap/Recovery Point process

Displays the name/path of the process that you want to run after the respective phase. You can use this space to enter a process that will execute after this phase on the subclient or Replication Set, or you can use the **Browse** button to search for and select the name/path of the process. The system allows the use of spaces in the name/path, provided they begin with an opening quotation mark and end with a closing quotation mark.

	If you are using the Linux File System *i*DataAgent to back up VMware virtual machines, you must create a PostBackup process script that will allow the system to post data back to the virtual machines. See "Create Pre/Post Backup Process Scripts to Back up VMware Virtual Machines Using the Linux File System *i*DataAgent" in Books Online for step-by-step instructions.

On Source

Specifies whether the PreSnap/PostSnap process will execute on the source computer.

On Proxy

Specifies whether the PreSnap/PostSnap process will execute on the proxy computer.

Run Post Backup/Scan/Migrate/Archive/Copy/Snap Process for all attempts

Specifies whether this process will execute for all attempts to run the phase. Selecting this option will execute the specified process for all attempts to run the phase, including situations where the job phase is interrupted, suspended, or fails. Otherwise, when the checkbox is cleared the specified process will only execute for successful, killed, or failed jobs.

On Primary Host/Backup Host/MediaAgent

Specifies the location of the batch file or shell script that you want to execute after a phase, either on the Primary Host (production server), Backup Host or MediaAgent.

Run As / User Account

Displays either the Local System Account, or for added security, another account as having permission to run these commands.

	SharePoint Server *i*DataAgent:
	Even if the Local System Account is selected as the account to run the Pre/Post processes, the account that actually will be used is the SharePoint Administrator Account for the site in which the SharePoint Server resides. This account was configured during installation and can be changed in Agent Properties.

Change

Click to add or modify the account that has permission to run these commands.

Browse

Click to search for and select the Pre/Post Process.

Encryption

Use this dialog box to select the data encryption options for the selected content. When accessing this dialog box from the Subclient Properties Encryption tab, this setting applies only to the selected subclient content for operations run from the CommCell Console. When accessing this dialog box from the Instance Properties Encryption tab, this setting applies only to third-party Command Line operations. The functionality is not propagated to the Subclient Properties Encryption tabs.

None

When selected, no encryption will take place during a data protection operations.

Media Only (MediaAgent Side)

When selected, for data protection operations, data is transmitted without encryption and then encrypted prior to storage. During data recovery operations, data is decrypted by the client.

When using this setting in conjunction with the client property **With a Pass-Phrase**, you will be required to provide a pass-phrase for data recovery operations unless you export the client pass-phrase to the destination client(s). When using pass-phrase security for third-party Command Line operations or DataArchiver Agents stub recovery operations, you must export the pass- phrase to the destination client.

Network and Media (Agent Side)

When selected, for data protection operations, data is encrypted before transmission and is stored encrypted on the media. During data recovery operations, data is decrypted by the client.

When using this setting in conjunction with the client property **With a Pass-Phrase**, you will be required to provide a pass-phrase for data recovery operations unless you export the client pass-phrase to the destination clients.

Network Only (Agent Encrypts, MediaAgent Decrypts)

When selected, for data protection operations, data is encrypted for transmission and then decrypted prior to storage on the media. During data recovery operations, data is encrypted by the MediaAgent and then decrypted in the client.

When using this setting in conjunction with the client property **With a Pass-Phrase**, you will not be required to provide a pass-phrase for data recovery operations.

Script Preview

Click to display the backup script, based on the current subclient configuration, that will be submitted to RMAN when backups are performed for the selected Oracle subclient.

Storage Device

Use this dialog box to establish the storage device related settings on the selected subclient. Note that all the options described in this help may not be available and only the options displayed in the dialog box are applicable to the agent or enabler for which the information is being displayed.

The following tabs are displayed:

- (Data) Storage Policy
- Data Transfer Option
- Deduplication

STORAGE POLICY

Use this tab to select or view storage policy settings on the selected subclient.

Data/Database/Transaction Log Storage Policy

Displays the storage policy to which this subclient is currently associated. To associate a storage policy to a new subclient or to change the storage policy associated with an existing subclient, click one in the list.

Incremental Storage Policy

Displays the name of the Incremental Storage Policy associated with this subclient, if the storage policy has the Incremental Storage Policy option enabled.

Data Paths

Click to view or modify the data paths associated with the primary storage policy copy of the selected storage policy.

Number of Data/Database/Transaction Log Backup Streams

Displays the number of streams used for backup operations. To change the number of streams, click one in the list. For DB2 DPF, be sure to set the appropriate number of streams for each database partition by double-clicking the appropriate **Stream** space and typing the desired number.

Client/Instance/Status/Stream

Displays the names of the instances according to current backup priority along with other associated information that are included in the Oracle RAC node. To change the backup priority of the instances, click the instance name as appropriate and use the directional arrows provided.

Maximum Backup Streams

For Informix, displays the maximum number of streams used for database backup operations, which is determined from the ONCONFIG file. The number of streams for backups cannot be set currently from the CommCell Console. Instead, you must set the BAR_MAX_BACKUP parameter in the $ONCONFIG file on the Informix client. Also, the number of streams specified by the storage policy must be greater than or equal to the number specified by the BAR_MAX_BACKUP parameter.

Data Threshold Streams

For Oracle RAC, specifies whether to run the backup job immediately when the total number of reserved streams is greater than or equal to the value in this field. If you click this option, use the space provided to change this value if desired.

Create Storage Policy

Click to launch the Create a Storage Policy wizard. Once the storage policy has been created, it will be displayed in the list of storage policies to which the selected subclient can be associated.

Buffer Size

Use this space to specify the size (in 4 KB pages) of each buffer to be used for building the backup image. The minimum value is 8, and the default value is 1024. If you select value 0, the value of the `backbufz` database manager configuration parameter will be used as the buffer allocation size.

DATA TRANSFER OPTION

Use this tab to establish the options for data transfer. Note that all the options described in this help may not be available and only the options displayed in the dialog box are applicable to the agent for which the information is being displayed.

Software Compression

Indicates whether software compression for the subclient or instance is enabled or disabled, and if enabled whether it is performed on the client or MediaAgent computer.

- **On Client**

  Click to enable software compression on the client computer.

- **On MediaAgent**

  Click to enable software compression on the MediaAgent computer.

- **Use Storage Policy Settings**

  Click to use the settings enabled on deduplicated storage policy copy.

  This option applies when subclient is associated with a storage policy copy that is deduplicated. See Copy Properties (Deduplication) - Advanced tab for compression settings on deduplicated storage policy copy.

- **Off**

  Click to disable software compression.

Note that hardware compression has priority over the software compression. Hardware compression is established in the Data Path Properties dialog box. The above software compression option will take effect when the data path is associated with a disk library, or when hardware compression is disabled in the data path associated with tape libraries.

For non-deduplicated storage policy copy, select **On Client** or **On MediaAgent** options to turn on compression, depending upon your environment.

Resource Tuning

Indicates the processes used by the client to transfer data based and whether bandwidth throttling is enabled or not.

- **Network Agents**

  Specifies the number of data pipes/processes that the client uses to transfer data over a network. Increasing this value may provide better throughput if the network and the network configuration in your environment can support it. On non-UNIX computers, the default value is 2 and a maximum of 4 can be established if necessary. On UNIX computers the default value is 1 and a maximum of 2 can be established if necessary.

- **Throttle Network Bandwidth (MB/HR)**

  Specifies whether the backup throughput is controlled or not. (By default this option is not selected and therefore the throughput is not controlled). When selected, use the space to specify a value for the throughput. By default, this is set to 500. The minimum value is 1 and there is no limit to the maximum value. (In this case the backup throughput will be restricted to the maximum bandwidth on the network.)

Use this option to set the backup throughput, based on the network bandwidth in your environment. Use this option to reduce the backup throughput, so that the entire network bandwidth is not consumed, especially in slow links. Increasing this value will end up consuming the bandwidth with the maximum throughput limited to the network bandwidth capability.

Note that throttling is done on a per Network Agent basis.

Application Read Size

This option specifies the amount of application data (such as SQL data, Windows File System data, and virtual machine data) backup jobs will read for each unit transferred to the MediaAgent.

The default value for this options is 64KB; however, this value may be increased to reduce the amount of data read from the given application, which in turn reduces the amount of I/O operations performed against it. As a result, overall backup performance may increase. However, backup memory usage may also increase, which may inadvertently consume additional resources from the application. Thus, it is recommended that this value be set at either the default value or match the block size directed by the application.

DEDUPLICATION

Use this tab to establish the options for deduplication on the subclient. It indicates whether deduplication for the subclient is enabled or disabled, and if enabled whether the signature generation (a component of deduplication) is performed on the client or MediaAgent computer.

Note that deduplication is supported on disk storage devices. So the deduplication options are applicable only if the subclient is associated with a Storage Policy containing disk storage.

On Client

Click to enable signature generation on the client computer.

On MediaAgent

Click to enable signature generation on the MediaAgent computer.

Back to Top

Subclient Properties (Content)

Use this tab to define the contents of a new subclient or to change the content of an existing subclient. Items included in subclient content are backed up/migrated/content indexed by the subclient. Note that all the options described in this help may not be available and only the options displayed in the dialog box are applicable to the agent for which the information is being displayed.

Contents of subclient

Displays a list of paths of data/workspaces/categories/documents/folders included as content for this subclient. Special characters (such as "\" "/" "." ",") represent content of the default subclient, that is not assigned to other subclients within the backup set. For Unix, when a symbolic link is included in the subclient content, the target of the symbolic link along with the link itself can be displayed.

- **Delete**

  Click to delete the selected path/data/folder from the Contents list for this subclient.

- **Browse**

  Click to browse for new content that you want to add to this subclient.

	When browsing content while configuring SharePoint subclients, you can add content via multiple selections with the CTRL or SHIFT keys.

- **Add Paths**

  Click to enter a new content path.

  Enter the UNC path of the share to configure a subclient to backup and restore.

	Type in the UNC path of the share that has to be added in the **Enter New Content** field and click **Add**. Repeat this step to add more files and/or folders to the content.
	1. If this is the first UNC path being entered as subclient content the **Impersonate NT User** dialog box will appear. Enter the user account information for the Domain User with permissions for that path. Note the following:
	○ Login name must be provided in the following format: <domain>\UserName
	For example, to log on as usr1 in a domain called MyDomain, enter **MyDomain\usr1** as the user name

	○ The domain user that you specify should have access to all the UNC paths entered as contents of the subclient. ○ Adding a UNC shared path as subclient content of a member server that points to a server in a workgroup requires the local user name and password is identical to a domain user's name and password. (This is a scenario where <UserName> and password is accepted.) ○ Adding a UNC shared path as subclient content of a non-member (workgroup) server that points to a member server requires the local user name and password is identical to a domain user's name and password. (This is a scenario where <UserName> and password is accepted.) ○ The domain user can be changed at a later time with the **As User** button. 2. To save your content changes, click **OK**.
	For File Archiver for Windows, UNC paths are not supported with subclients associated with Local File System.

- **As User**

  Click to enter/modify the User Name and Password required to access the UNC path when a UNC path is entered as content.

Discover

Click to display the data paths to which the symbolic links in the data contents are pointing. The paths will be displayed in **Contents of subclient**. This button is enabled only when **Expand symbolic links of subclient content** below is enabled.

	Instead of clicking **Discover**, wait until the backup completes and then refresh the subclient. Then go to **Contents of subclient**. The data contents for the symbolic links should be displayed.

Perform backup using mining off snapshot

Click to run a data protection job from an offline copy of a SharePoint database. The offline copy is created by using the SQL Server iDataAgent to create a SnapProtect backup. Snap mining can improve performance in that it offloads processing on the production application server since processing calls are not required from the SharePoint Server during backup.

SQL DB client

Specifies the client computer where the SharePoint Database and SQL Server iDataAgent is installed.

Agents

Specifies the SQL Server iDataAgent that was used to create the SnapProtect backup of the SharePoint Database.

Instance

Specifies the instance of the SQL Server *i*DataAgent that was used to create the SnapProtect backup

SQL DB subclient to use

Specifies the subclient to use for mining the SnapProtect backup.

Proxy Client

Click if you want the data protection job of the SnapProtect backup to run on the Proxy Client. Then specify the computer for the Proxy Client.

Configure

Click to discover and change the associations of the mailboxes to the subclients. Any mailboxes included as content for a user-defined backup set/subclient will be automatically excluded from the default backup set/subclient.

Backup Content Path

Click the drop-down list arrow to display the root volumes on the file server. To change the root volume, click one in the list. If you want to refine the content path further, use the space to the right of (or below) the root volume list to enter additional path information. Note the following:

- For NetApp, the root volume is the mount path of each volume.
  Example: for volume `FS1` the root volume will be `/vol/FS1`.

- For EMC Celerra, the root volume is the mount point created for a volume.
  Example: for volume `FS1` with mount point `/FS1` the root volume will be `/FS1`.

- For Hitachi, no root volumes are shown in the drop down list. Type the full path of the root volume.
  Example: for volume `FS1` with mount point `/mnt/FS1` the root volume will be `/mnt/FS1`.

- For BlueArc, the root volume is a combination of a descriptor of the path and the volume name.
  Example: for volume `FS1` with a mount point of `/` the root volume will be `/__VOLUME__/FS1`.

For Celerra tape silvering, specify the source path of the replication that was created from the Celerra Management Console or command line. Append `.ts` to the path name. For example, `/sourcefs/.ts`.

Enter new content

Use this space to specify the paths of other data that you want the subclient to contain.

Add

Click to add the data that you specified in **Enter new content** or **Backup Content Path** to the Contents list.

Treat characters as regular expressions

Specifies whether regular expressions (i.e., strings that use wildcard characters) will be interpreted as wildcards or as literal strings. Select this option to recognize wildcard characters in the content path. See Wildcards for a list of supported wildcards.

Case Sensitive

Specifies whether content paths will be case sensitive. Selecting this option will cause the system to recognize the difference between upper case and lower case characters in the content path.

Backup System State

Specifies whether the system state will be backed up with this subclient. Selecting this option causes the system state to be backed up with the file system for this subclient.

Backup Office Communication Server

Specifies whether the Office Communications Server will be backed up with this subclient. Selecting this option causes the OCS data & settings to be backed up with the file system for this subclient.

- **Edit**

  Click to enter/modify the User Name and Password required to access the Office Communications Server.

Only backup files that qualify for archiving

Click to backup only those files within the specified content, which meets the archiving rules.

Enable Apple Double Support

Specifies whether to facilitate the management of resource fork data in Apple Double-encoded Macintosh files.

	This option may not work on Solaris subclients.

Expand symbolic links of subclient content

Specifies whether to display the data paths to which the symbolic links (if any) in the subclient content are pointing. Whenever this option is enabled, the **Discover** button discussed above is enabled and used to this purpose.

Back to Top

Browse Options

Use this dialog box to select the basic options under which you want to browse the data secured by a data protection operation in the selected client, agent, instance/partition, or backup set level depending on the functionality of a given agent.

The system provides several browse options. These options influence the behavior of the browse operation in the subsequent Browse window. Note that all the options described in this help may not be available and only the options displayed in the dialog box are applicable to the agent for which the information is being displayed.

Browse the Latest Data

Specifies whether the browse operation must display data from the most recent data protection operation (from now back to the last full backup) in the Browse window. (This option is selected by default.)

Specify Browse Time

Specifies whether the browse operation must display data, up to the specified date and time in the Browse window. Data secured after the specified date and time will be omitted in this window.

- **Browse Data Before/Browse to Point-In-Time**

  Specifies the date and time that must be used to display the data in the Browse window.

- **Time Zone**

  Lists the time zones. To change the time zone, click one in the list.

Select from Available Browse Times

Displays a list containing the time of different backup jobs available in the destination, from which data can be browsed. For Workstation Backup Agent, this option displays the list of recovery points available in the destination. Select the desired time.

Use MediaAgent

Specifies the name of MediaAgent that will be used to perform the browse (and restore) operation. If necessary, you can change the name of the MediaAgent. For example, if the library is shared and you wish to use a specific MediaAgent (instead of the system selected MediaAgent, or a MediaAgent which may be idle,

or less critical) or if you know that the media containing the data you wish to restore is available in the library attached to the specified MediaAgent.

If the media containing the data is not available in the tape/optical library attached to the MediaAgent, the system will automatically prompt you to insert the appropriate media. In the case of a disk library, the operation will fail if the requested data is not available in the disk library attached to the specified MediaAgent.

Client Computer

Lists the client computers available for the browse operation. This option is available only when the browse operation is performed either from the client node in the CommCell Browser, **Browse & Recover** option from the **Tools** menu in the CommCell Console or when the **New Browse** button is clicked in the Browse window.

Specify Browse Path

Specifies the starting point for the browse operation. Also provides a space for you to type the path.

Show Deleted Items

Specifies whether the operation will browse all the data (including deleted items) secured by all data protection operations for the selected backup set as of the specified browse items.

Table View

Specifies whether the backup data should be displayed as database tables during the browse operation.

Image Browsing

Specifies whether the operation will browse all the data (including deleted items) secured by all data protection operations for the selected backup set as of the specified browse times.

The main difference between image browse and no-image browse is that deleted items are shown only by the no-image browse.

Keep in mind that the display of deleted items depends on whether full backup transparency is enabled. If full backup transparency is disabled (the default), only those deleted items that existed back through the most recent full backup are shown. However if full backup transparency is enabled, the deleted items shown includes those that existed during the time interval from initial index creation through the time being browsed.

To determine whether full backup transparency is enabled or disabled, from the CommCell Browser, right-click the *i*DataAgent and then select **Properties.** Click the **Index** tab. If **Create new index on full backup** is selected, then full backup transparency is disabled.

File Level Browse (Restore individual files/folders from disk image)

Specifies whether the operation will browse all the files and folders secured by all data protection operations for the selected backup set as of the specified browse items.

Volume Level Browse (Restore the disk image/volume)

Specifies whether the operation will browse all the volumes secured by all data protection operations for the selected backup set as of the specified browse items.

Database

For SQL Server, specifies whether to browse individual databases.

File/File Group

For SQL Server, specifies whether to browse file groups and files for the databases.

Page Size

Use the space to enter the default number of objects to be displayed in the Browse window. This field reverts back to the default setting after use. In the Browse window, you can browse through each page list by selecting the appropriate page number.

Browse Data from SQL

Specifies that SharePoint documents can be mined from an offline mining database.

SQL Instance

For SharePoint Offline mining, specifies the SQL instance that is associated with the offline mining database. Click ... to select from a list or type the instance name.

User Account

For SharePoint Offline mining, specifies the Username and Password of the account that can access the instance. Click Edit to enter the username and password.

Config Database

For SharePoint Offline mining, specifies the Configuration Database that will be used to mine SharePoint documents. Click ... to select from a list or type the Configuration Database name.

Browse only volumes

Specifies that the browse operation must display only a list of volumes; required for a Volume Level Restore.

Advanced

Click to access additional browse capabilities.

List Media

Click to display media required for restore or index restore operations.

Type of Intended Restore (Virtual Server *i*DataAgent)

This section provides the facility to select the type of restore you want to perform following the Browse operation.

● **Individual Files/Folders**

Select this option if you intend on performing a file/folder-level restore.

● **Entire Volume**

Select this option if you intend on performing a volume-level restore.

● **Container Restore**

Select this option if you intend on performing a disk-level restore.

Browse/Restore Directory Server data from database

For Active Directory Offline Mining, enter the path to the database from which you want to restore directory server data. For Active Directory Server databases, this file will be the `ntds.dit` file. For ADAM and Lightweight Server databases, this file will be the `adamntds.dit` file. Click **Browse** to locate the database or enter the complete database path in the **File Path** field.

Advanced Browse Options

Use this dialog to access additional browse capabilities for the browse window. Note that all the options described in this help may not be available and only the options displayed in the dialog box are applicable to the agent for which the information is being displayed.

Use MediaAgent

Select the MediaAgent associated with the data you want to browse, or select **Any MediaAgent**.

Show Deleted Items

Specifies whether the operation will browse all the data (including deleted items) secured by all data protection operations for the selected backup set as of the specified browse items.

Page Size

Specifies the number of objects to be displayed in the browse window.

Include Metadata

Specifies that the browse operation results must also include data containing metadata information.

Exclude Data Before

Specifies that the browse operation must return data that has been backed up after the specified date. Also provides a space for you to type the date and time.

Browse from copy precedence

When selected, the system retrieves the data from the storage policy copy with the specified copy precedence number. If data does not exist in the specified copy, the operation fails even if the data exists in another copy of the same storage policy.

When cleared, (or by default) the system retrieves data from the storage policy copy with the lowest copy precedence. If the data was pruned from the primary copy, the system automatically retrieves the data from the other copies of the storage policy starting with the copy with the lowest copy precedence and proceeding through the copies with higher copy precedence. Once the data is found, it is retrieved, and no further copies are checked.

List Media

Use this dialog box to select the options that must be used to predict the required media.

Media For the Latest Data

Specifies whether the list media operation must display media associated with the most recent data protection operation (from now back to the last full backup) This option is selected by default.

Specify Time Range

Specifies whether the whether the list media operation must display media associated with the specified date and time.

- **Data Before/Time Range**

  Specifies the date and time that must be used to display media.

- **Time Zone**

  Lists the time zones. To change the time zone, click one in the list.

Advanced

Click to access additional options.

Restore by Jobs Filter

Use this dialog box to establish filtering options for the Restore by Jobs feature. The available options are:

Specify jobs from list

Specifies that you will be able to select one or more jobs from the Backup History dialog box based on a fixed time range for the jobs that you specify by using the **Absolute** option below. Backup jobs whose start and end times fall within this time range will be selected and eligible for restore. This option is selected by default and, when selected, the **Absolute** option within **Time Range** is automatically selected. Once you make all of your selections on this dialog box using all these options and click **OK**, the Backup History dialog box displays. From this dialog box, you can specify the actual job(s) to restore.

Specify time range

Specifies that all eligible jobs will be selected based on the relative time range that you specify for the jobs by using the **Relative** option below. Backup jobs that were completed within the time range indicated relative to when the restore will start will be eligible for restore. When you select this option, the **Relative** option within **Time Range** is automatically selected. Once you make all of your selections on this dialog box using all these options and click **OK**, the Restore Options for All Selected Items dialog box displays.

Backup Type

Displays the types of backup jobs that can be restored. Select one of the following:

- **All**

  Specifies that all backup jobs should be restored.

- **Full**

  Specifies that all full backup jobs should be restored.

- **Differential**

  Specifies that all differential backup jobs should be restored.

- **Incremental**

  Specifies that all incremental backup jobs should be restored.

- **Synthetic Full**

  Specifies that all synthetic full backup jobs should be restored.

Job Status

Displays only those jobs that correspond to a specified job status. Select one of the following:

- **All**

  Displays all jobs.

- **Completed**

  Displays only jobs that completed and completed with one or more errors.

- **Failed**

  Displays only those jobs that were killed, failed, and failed to start.

- **Killed**

  Displays only user killed jobs.

Time Range

Use this area to select the jobs to restore based on different time criteria.

- **Absolute**

  This option is automatically selected when you select **Specify jobs from list** above. Select from the following two options:

  Time Zone

  Displays only those jobs that have occurred within a specified time zone.

  Start Time, End Time

  Displays only those jobs that occurred within the specified start and end times.

- **Relative**

  This option is automatically selected when you select **Specify time range** above. Use the spaces to select the relative time period for the restore job(s).

Advanced

Click to administer additional backup history filter options.

Back to Top

Operation Window

Use this dialog box to add, modify, or delete operation rules for system operations.

Name

The friendly name assigned to the operation window.

Operations

The operations included in the rule.

Days

Displays the days in which the operations in this rule should not be run.

Do not run intervals

Displays the times in which the operations in this rule should not be run.

Add

Click this button to add an operation rule from the Operation Rule Details dialog box.

Modify

Click this button to modify an operation rule from the Operation Rule Details dialog box.

Delete

Click this button to delete an operation rule.

Ignore Operation Rules at Higher Levels (not applicable at the CommServe and Client group level)

Select this option to disable all operation rules set at levels above the currently selected entity.

Getting Started - File Archiver Configuration

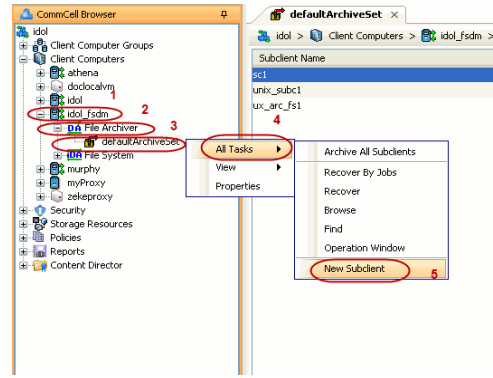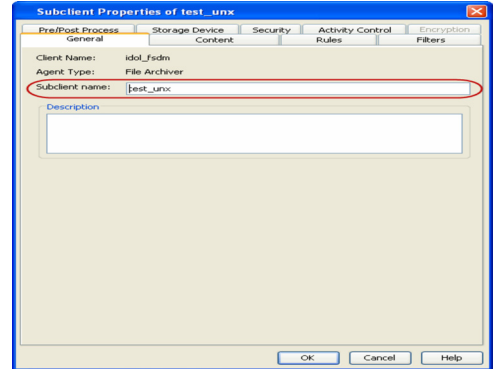◀ Previous   Next ▶

CONFIGURATION

Once the Unix File Archiver Agent has been installed, configure a Subclient to facilitate archiving. The following sections provide the necessary steps required to create and configure a subclient for running the first archive job.

1.
- From the CommCell Browser, navigate to **<Client> | File Archiver | Default Archive Set**.
- Right-click **Default Archive Set | All Tasks**
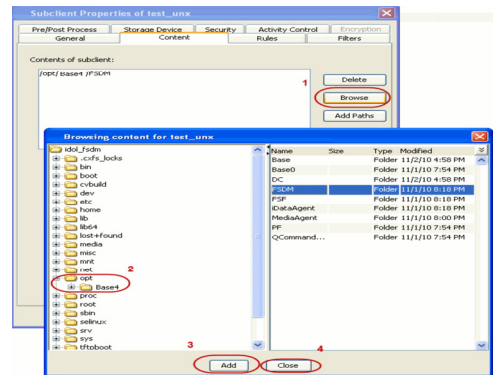- Click **New Subclient**.

2.   Enter **Subclient Name**.

3.
- Click the **Content** tab.
- **Browse** to the folder that has files to be archived.
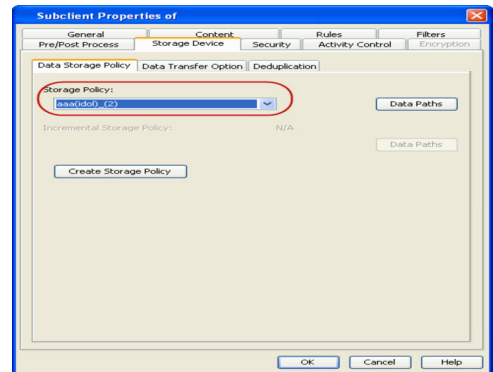- Select the folder and click **Add.**
- Click **Close**.

4.
- Click the **Storage Device** tab.
- Select the **Storage Policy** from the drop down list.
- Click **OK**.

If you do not have a Storage Policy created, follow the steps given below to create a Storage Policy.

5.
1. Click **Create Storage Policy**.

2. Follow the prompts displayed in the Storage Policy Wizard. The required options are mentioned below:
    ○ Select the Storage Policy type as `Data Protection and Archiving`.
    ○ Select `No` to allow legal hold to use the policy.
    ○ Specify the name of the Storage Policy.
    ○ Specify the name of the primary copy. The primary copy is automatically created along with the Storage Policy.

○ Select No for use of an existing global deduplication policy.

○ Specify name of the default library to which the Primary Copy should be associated. This must be a disk library. Ensure that you select a library attached to a MediaAgent operating in the current release.

○ Select the MediaAgent.

○ Verify the device streams and the retention criteria information.

○ Select Yes to enable deduplication for the primary copy. Select the Enable Client Side Deduplication option.

○ Name of the Deduplication Store, MediaAgent hosting the Deduplication Store, and the location of the Deduplication Store.

○ Review the details and click **Finish** to create the Storage Policy. The primary copy is also created.