Administration Guide - NetApp File Archiver

TABLE OF CONTENTS

MIGRATION ARCHIVING - NETAPP FILE ARCHIVER AGENT

RECOVER DATA - NETAPP FILE ARCHIVER AGENT

DATA AGING- FILE ARCHIVER FOR NETAPP

ADDITIONAL OPERATIONS- NETAPP FILE ARCHIVER AGENT

TROUBLESHOOTING - NETAPP FILE ARCHIVER AGENT

Overview - NetApp File Archiver Agent

TABLE OF CONTENTS

INTRODUCTION

File Archiver for NetApp Agent is installed as a stand alone archiving agent to archive and recover data residing on a NetApp File Server. The Data is always archived on CIFS share.

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 NetApp 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 NetApp 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 NetApp 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 NetApp File Archiver documentation uses the following terminology:

PROXY CLIENT	A proxy client is any computer on which the File Archiver Agent is installed to archive and recover data residing on a NetApp File Server.
MIGRATION ARCHIVING	Migration archiving is a process of periodically moving unused or infrequently used NetApp 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: Windows Terminal or Console window.
STUB RECOVERY	If the subclient is configured to create stubs, you can perform a recall operation from a Windows 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.
PERSISTENT RECOVERY	Multiple stub recoveries are submitted to the Job Controller as one job called a Persistent Recovery job. The job will wait for approximately 5 seconds in order to allow other stub recovery requests being submitted on the same client to be batched into the same job.

Getting Started - NetApp File Archiver Agent Deployment

WHERE TO INSTALL

Install the software on a computer with connectivity to the NetApp File Server. The client computer must satisfy the minimum requirements specified in the System Requirements.

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.

PREREQUISITES

Ensure the following:

● User has administrative privileges on the NetApp File Server.

● User has administrative privileges on the computer where NetApp File Archiver agent will be installed.

METHOD 1: INTERACTIVE INSTALL

1. Run **Setup.exe** from the **Software Installation Disc** on a client computer.
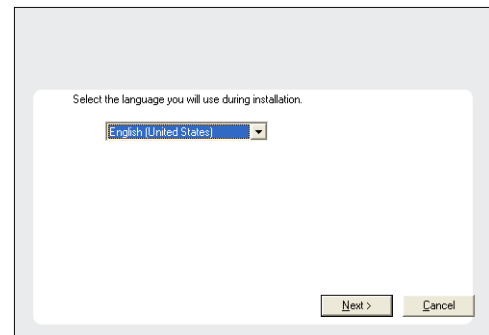
2. Select the required language.

   Click **Next**.

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

   The options that appear on this screen depend on the computer in which the software is being installed.
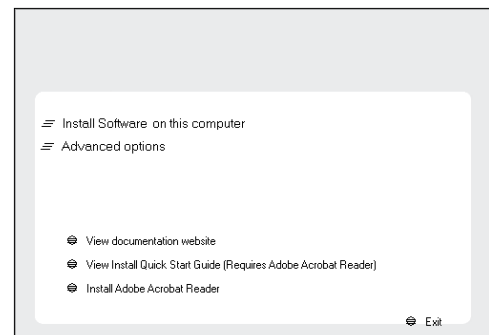
4. Select **I accept the terms in the license agreement**.

   Click **Next**.

5. Expand **Client Modules** | **Archive Management** and select **File Archiver for Windows Agent**

Click **Next**.

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

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

If firewall configuration is not required, click **Next**.
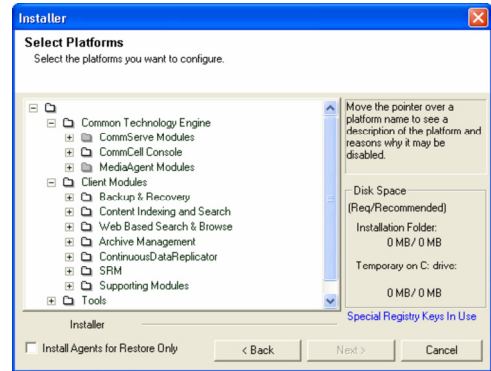
7. Enter the fully qualified domain name of the **CommServe Host Name**.

Click **Next**.

Do not use space and the following characters when specifying a new name for the CommServe Host Name:

\|`~!@#$%^&*()+=<>/?,[]{}:;'"
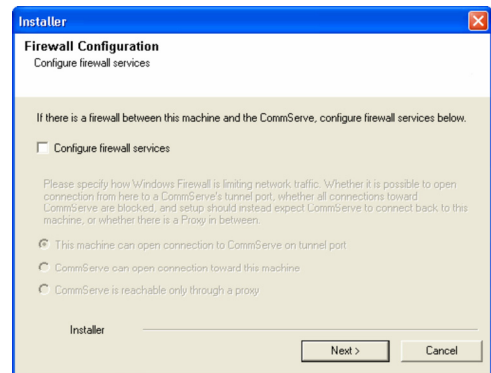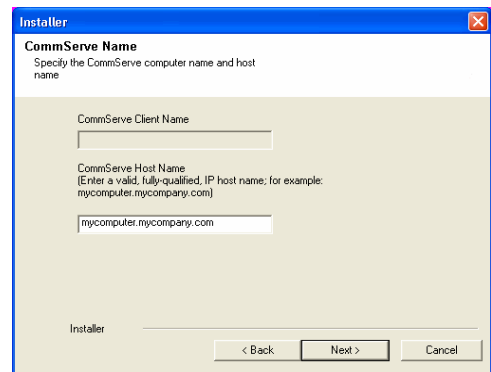
8. Click **Next**.

9. Select **Add programs to the Windows Firewall Exclusion List**, to add CommCell programs and services to the Windows Firewall Exclusion List.

    Click **Next**.

    > This option enables CommCell operations across Windows firewall by adding CommCell programs and services to Windows firewall exclusion list.
    >
    > It is recommended to select this option even if Windows firewall is disabled. This will allow the CommCell programs and services to function if the Windows firewall is enabled at a later time.

10. Verify the default location for software installation.

    Click **Browse** to change the default location.

    Click **Next**.

    - Do not install the software to a mapped network drive.
    - Do not use the following characters when specifying the destination path:

      / : * ? " < > | #

      It is recommended that you use alphanumeric characters only.

11. Select a Client Group from the list.

    Click **Next**.

    > This screen will be displayed if Client Groups are configured in the CommCell Console.

12. Click **Next**.
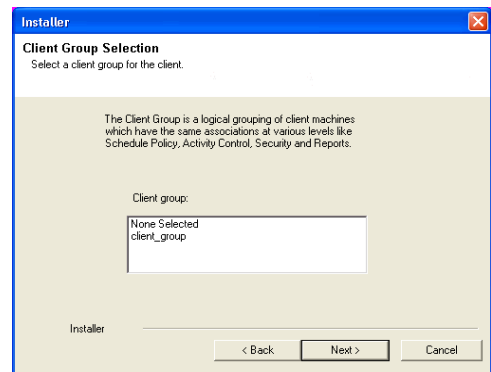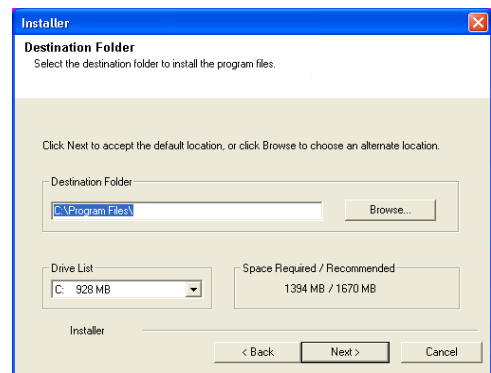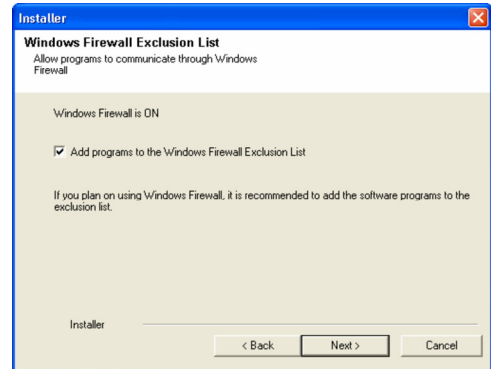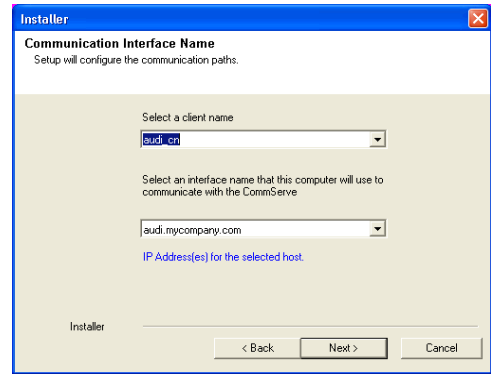
If you do not have Storage Policy created, this message will be displayed.

Click **OK**.

You can create the Storage Policy later in step 16

13. Click **Next**.

14. Click **Next**.

15. Click **Finish**.
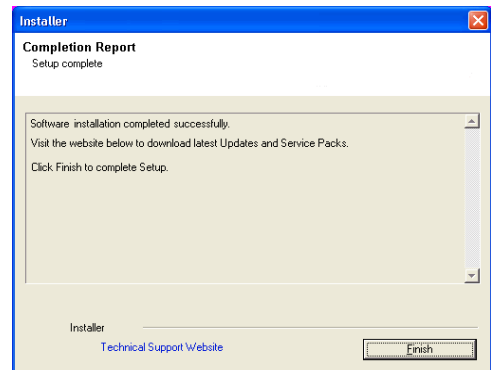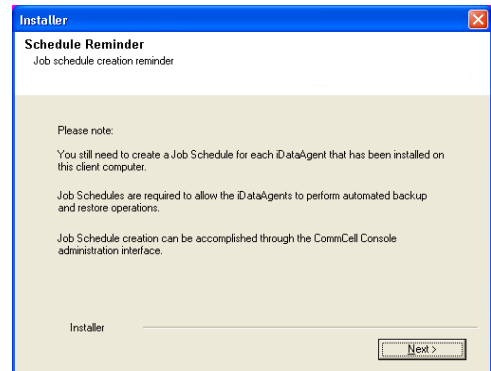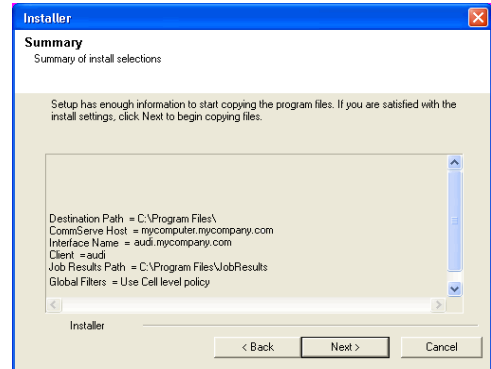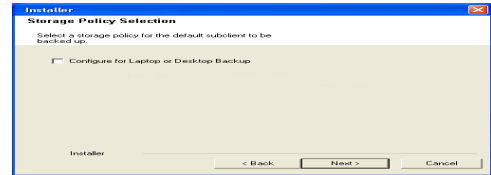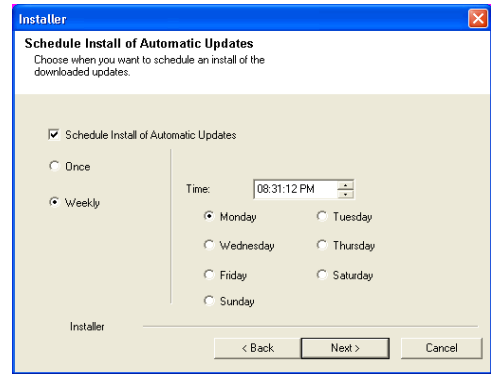
If you already have a storage policy selected in step 12, click the **Next** button available on the bottom of the page to proceed to the **Configuration** section.

If you do not have Storage Policy created, continue with the following step.

16. Create a Storage Policy:

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.
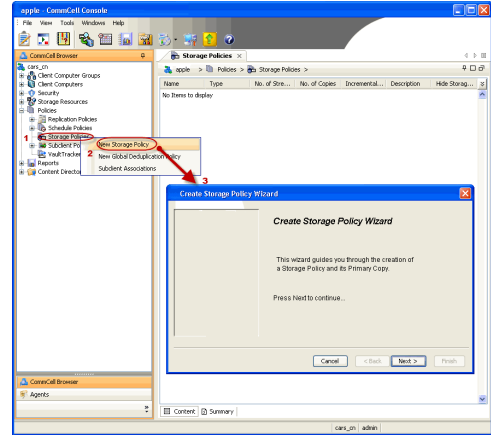
METHOD 2: INSTALL SOFTWARE FROM COMMCELL CONSOLE

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

2. Click **Next**.

3. Select **Windows**.

Click **Next**.
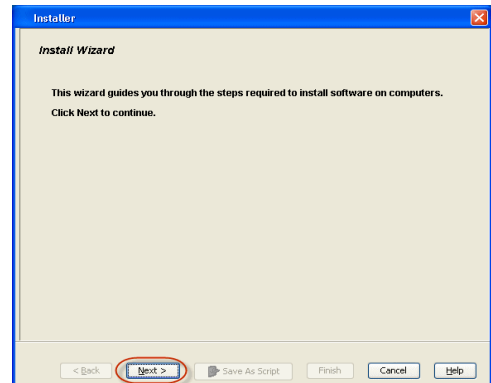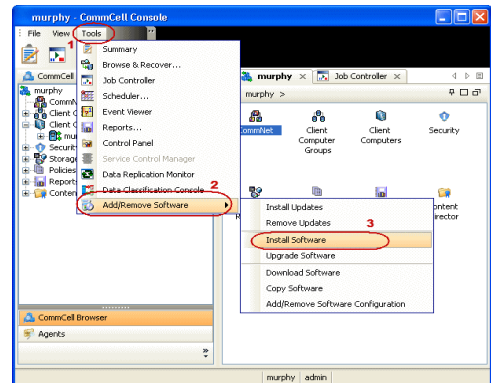
4. Select **Manually Select Computers**.

   Click **Next**.
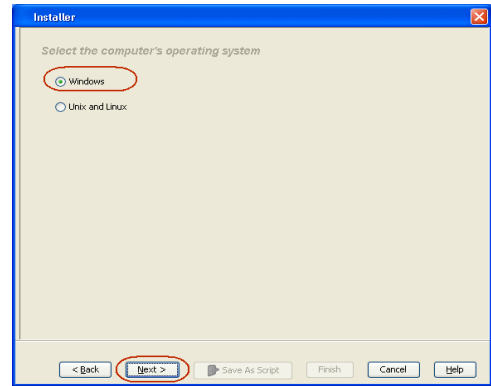
5. Enter the fully qualified domain name of the client computer.

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

   Click **Next**.
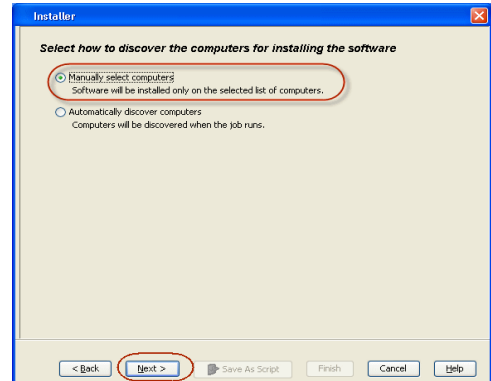
6. Click **Next**.
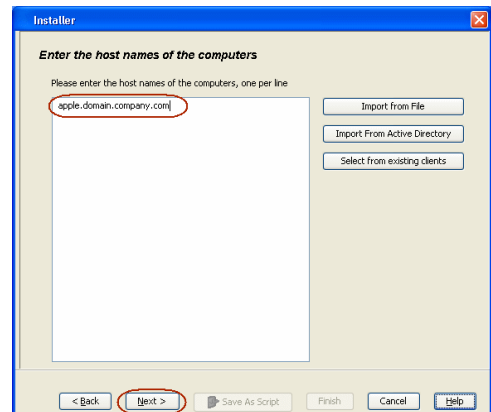
7. Specify **UserName** and **Password** of the client computer.

   Click **Next**.
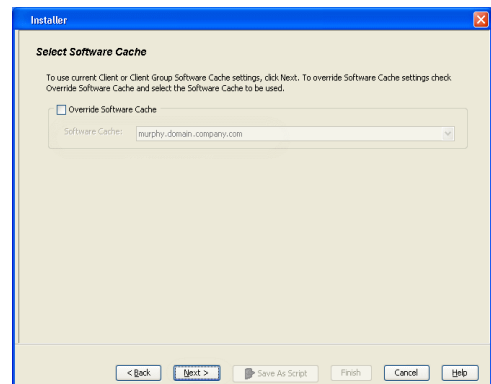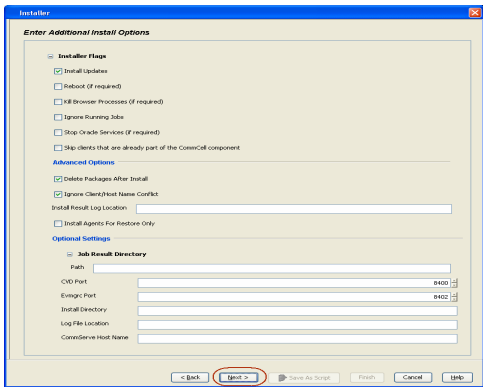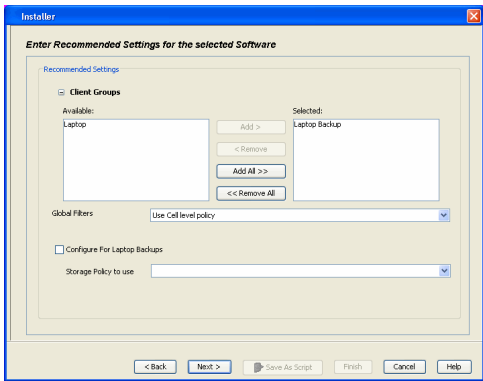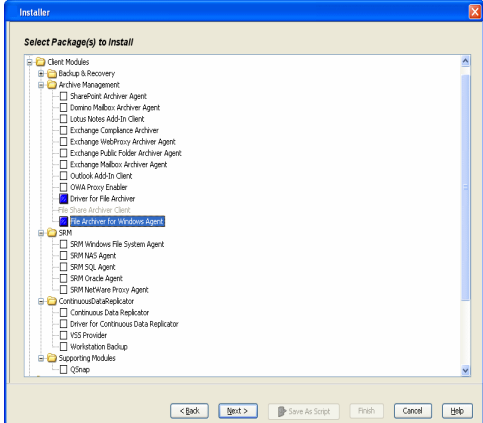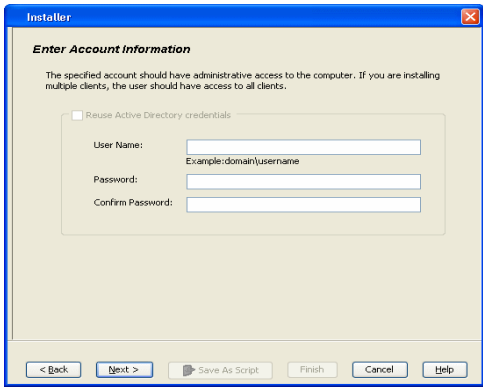
8. Select **File Archiver for Windows Agent**.

Click **Next**.

9.
- Select **Client Group** from **Available** and click **Add.**
- Select Storage Policy from **Storage Policy to use** drop-down list.
- Click **Next**.

10.
- Select **Reboot.**
- Click **Next**.

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

12. Click **Finish**.
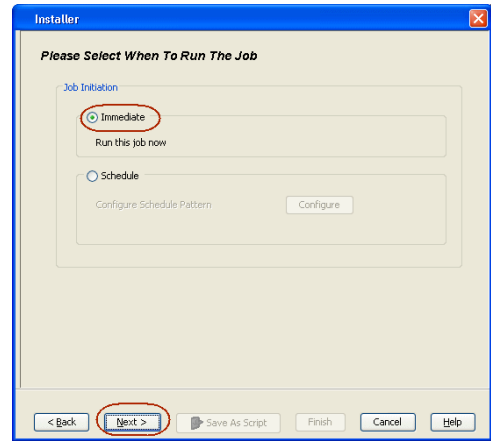
13. You can track the progress of the job from the **Job Controller** or **Event Viewer** window.
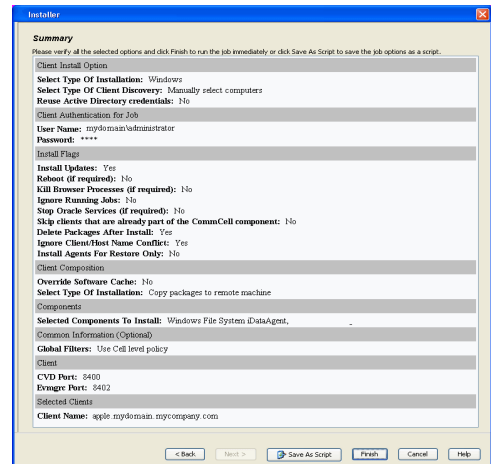
14. Once the job is complete, right-click the **CommServe** computer, click **View** and then click **Admin Job History**.
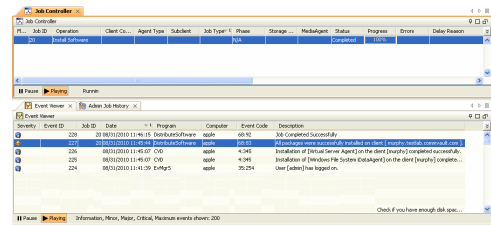
15. Select **Install/Upgrade/Remove Software**.

Click **OK**.
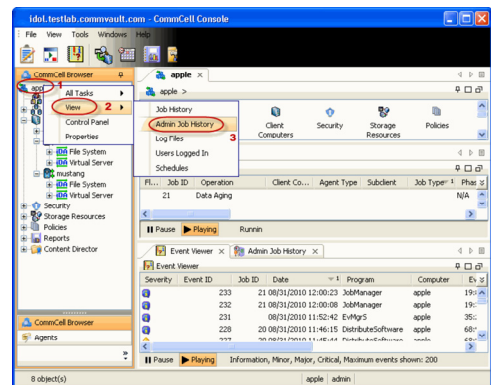
16. You can view the following details about the job by right-clicking the job:
    ● Event of the job displaying that the software installation has started and completed.
    ● Details of where the job was run.
    ● Date of the job.
    ● Client computer name on which the software was installed.
    ● Logs of the job.
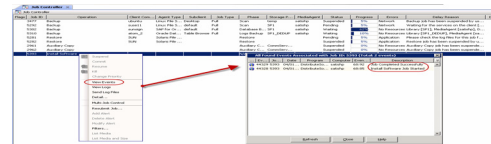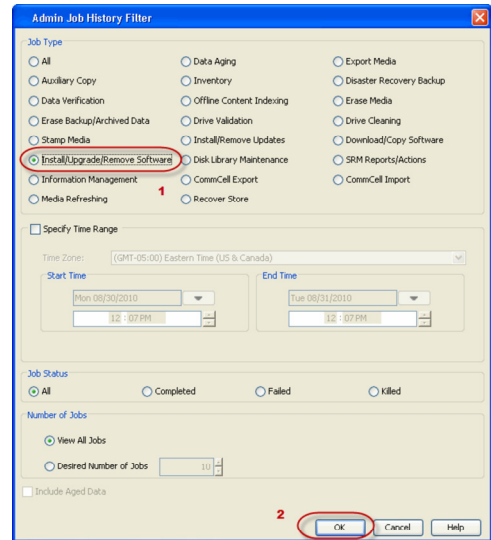
Getting Started - NetApp File Archiver Agent Deployment on a Cluster

SKIP THIS PAGE IF YOU ARE NOT INSTALLING THIS AGENT ON A CLUSTER.

Click Next ▶ to continue with the deployment.

WHERE TO INSTALL

Install the software from the active node in the cluster group. The driver for the File Archiver Agent must be installed onto all the physical nodes of the cluster. Once the driver is installed, 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.

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.

PREREQUISITES

Ensure the following:

- User has administrative privileges on the NetApp File Server.
- User has administrative privileges on the computer where NetApp File Archiver agent will be installed.

1. Run **Setup.exe** from the **software installation package** on a client computer.

2. Select the required language.

    Click **Next**.

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

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

4. Click **Next**.
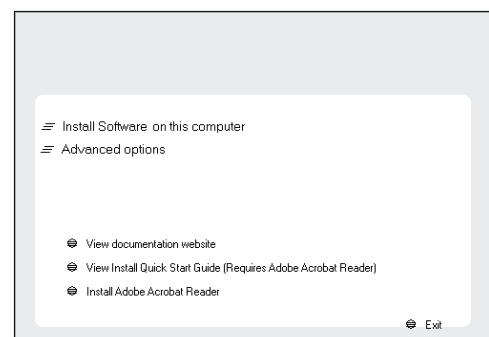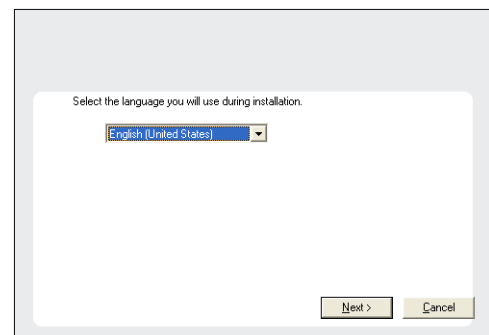
5.   Click **OK**.

6.   Select **I accept the terms in the license agreement**.

Click **Next**.

7.   Select **Install on the Physical Node**.

Click **Next**.

8.   Expand **Client Modules** | **Archive Management** and select **Driver for File Archiver.**

Click **Next**.

9.   If this computer is separated from the CommServe by firewall(s), type **Yes** and then press **Enter**.
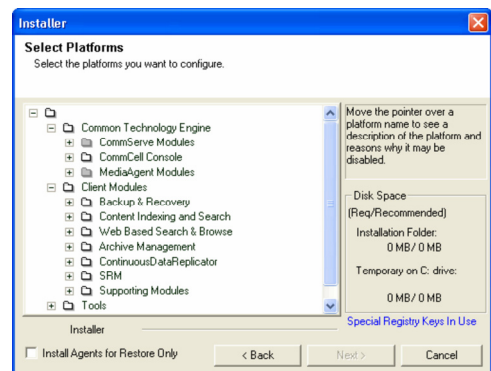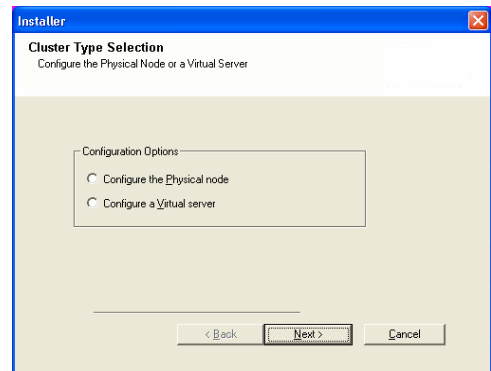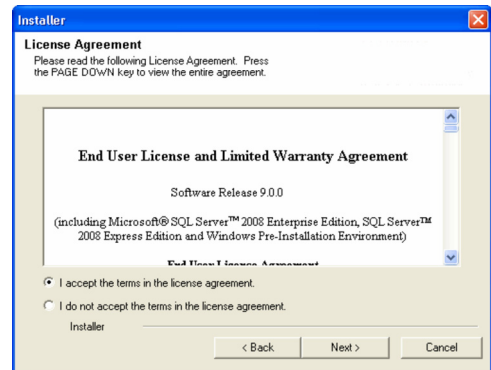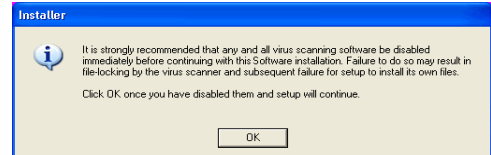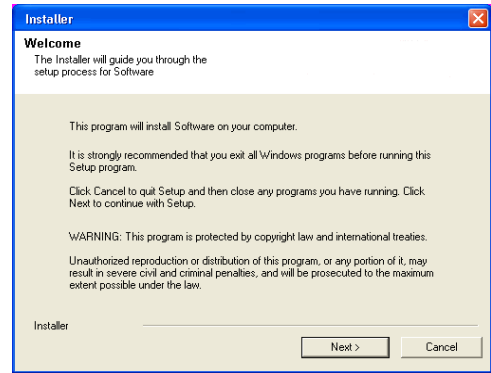
For firewall options and configuration instructions, see Firewall Configuration and continue with the installation.

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

10. Enter the fully qualified domain name and Click **Next**.

- Do not use space and the following characters when specifying a new name for the CommServe Host Name:

\|`~!@#$%^&*()+=<>/?,[]{}:;'"

11. Click **Next**.

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

Click **Next**.

This option enables CommCell operations across Windows firewall by adding CommCell programs and services to Windows firewall exclusion list.

It is recommended to select this option even if Windows firewall is disabled. This will allow the CommCell programs and services to function if the Windows firewall is enabled at a later time.

13. Click **Next**.

It is recommended to select the **Download latest update pack(s)** option to automatically install the available updates during installation.
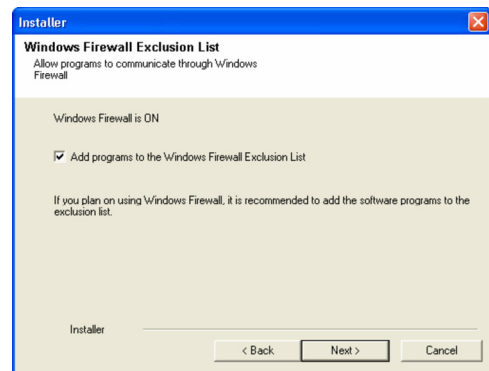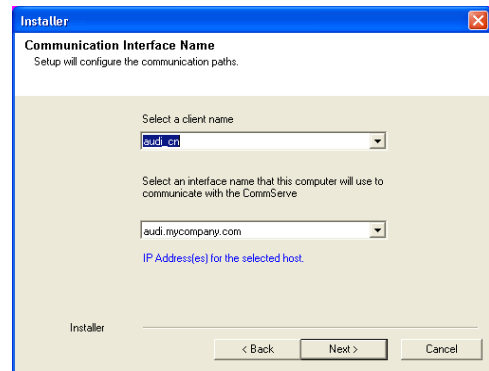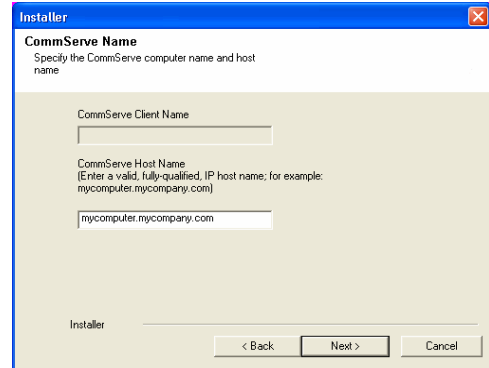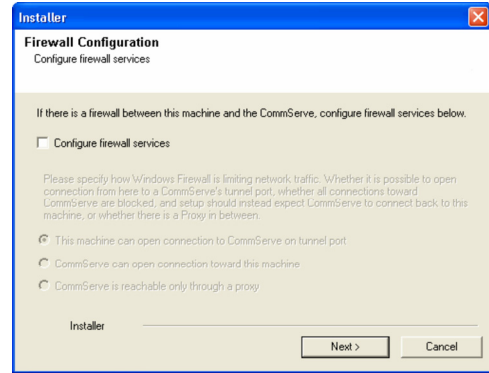
14. Verify the default location for software installation.

Click **Browse** to change the default location.

Click **Next**.

- Do not install the software to a mapped network drive.
- Do not use the following characters when specifying the destination path:

  / : * ? " < > | #

  It is recommended that you use alphanumeric characters only.

15. Select a Client Group from the list.

Click **Next**.

This screen will be displayed if Client Groups are configured in the CommCell Console.

16. Click **Next**.

17. Click **Next**.
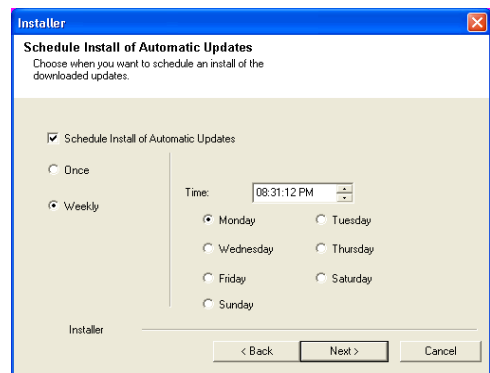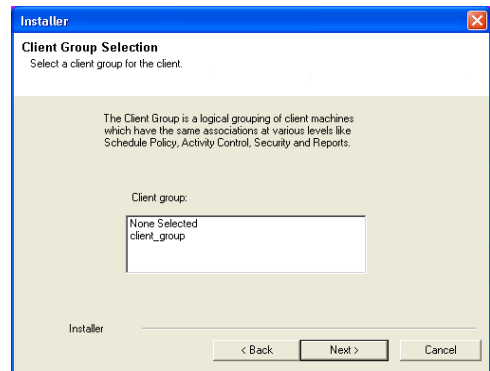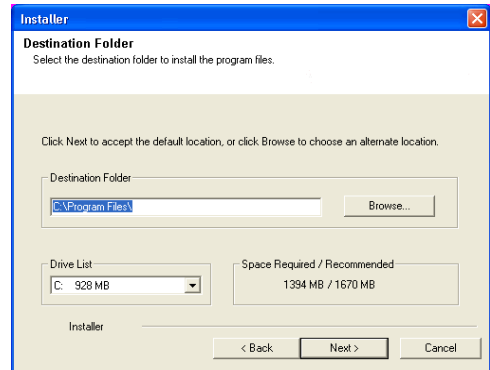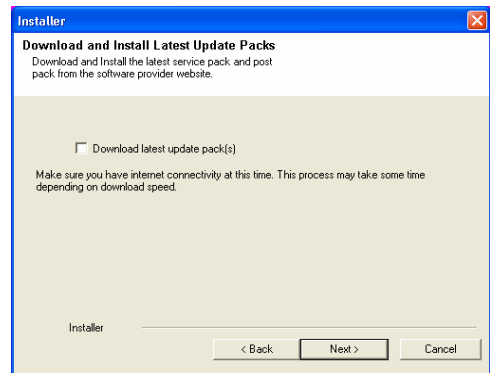
18. To install the software on the remaining nodes of the cluster, click **Yes**.

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

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

Once you complete your selections, click **Next**.

● The list of **Preferred Nodes** displays all the nodes found in the cluster; from this list you should only select cluster nodes configured to host this cluster group server.
● Do not select nodes that already have multiple instances installed.

20. Specify **User Name** and **Password** for the **Domain Administrator account Information** to perform the remote install on the cluster nodes you selected in the previous step.

Click **Next**.

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

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

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

● Maximum number of nodes on which Setup can run simultaneously.
● Time allocated for Setup to begin executing on each node, after which the install attempt will fail.
● Time allocated for Setup to complete on each node, after which the install attempt will fail.
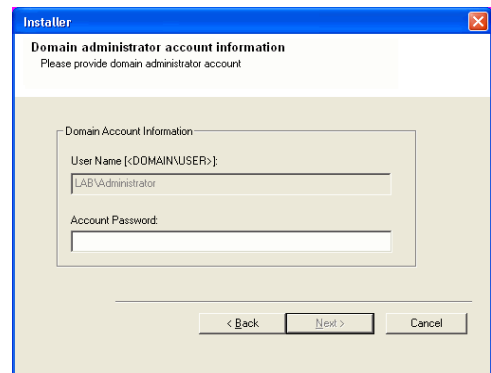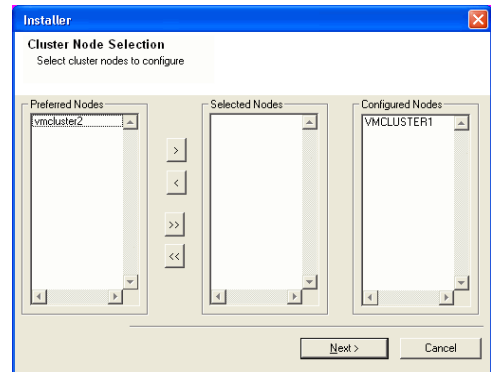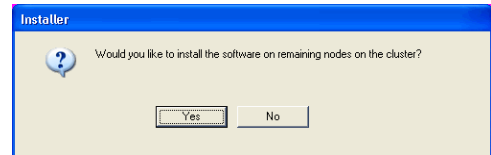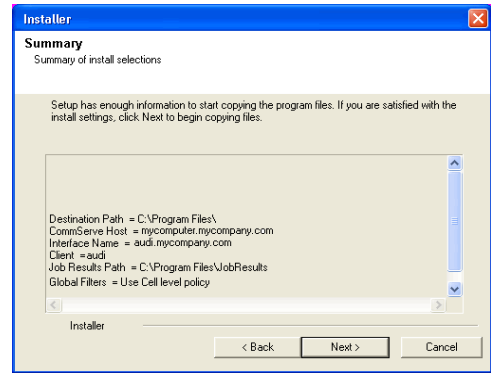
22. Read the summary for remote installation to verify that all selected nodes were installed successfully.

Click **Finish**.

- If, during the remote install of a cluster node, setup fails to complete or is interrupted, you must perform a local install on that node. When you do, the install begins from where it left off, or from the beginning if necessary. For procedures. follow from Step 1.

23. Click **Finish**.

24. Run **Setup.exe** from the **software installation package** on a client computer.

25. Select the required language.
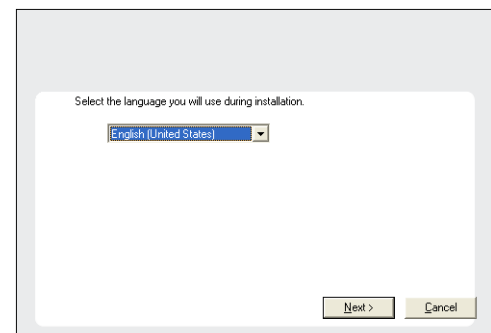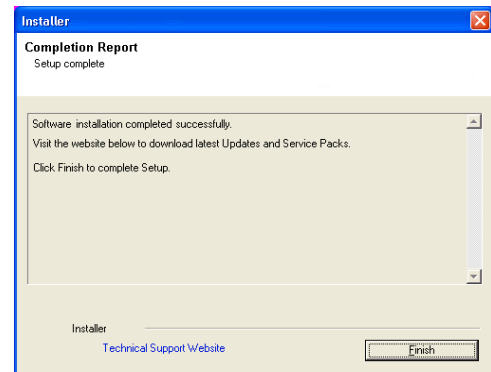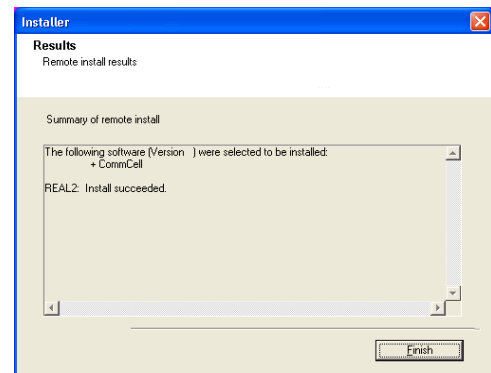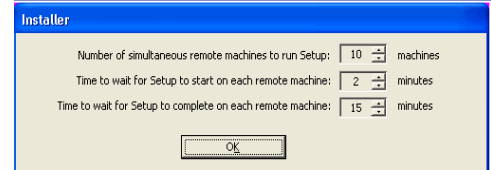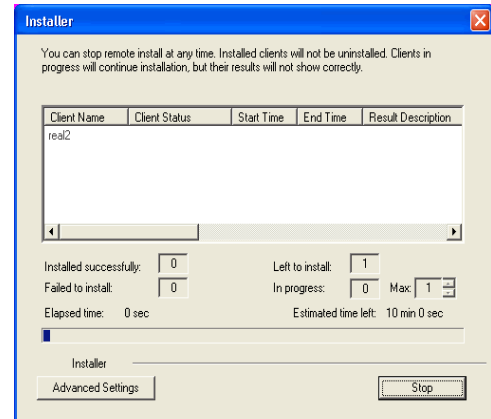
Click **Next**.

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

The options that appear on this screen depend on the computer in which the software is being installed.
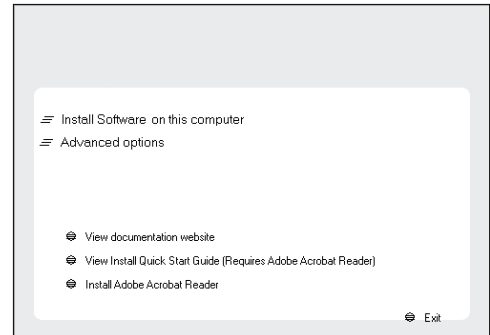
27. Click **Next**.
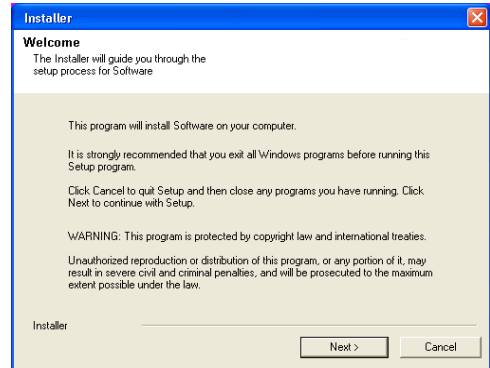
28. Click **OK**.
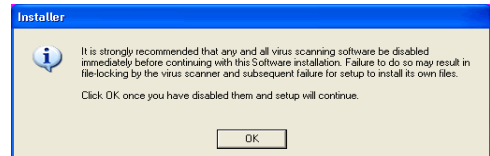
29. Select **I accept the terms in the license agreement**.

Click **Next**.

30. Select **Configure a Virtual Server**.

Click **Next**.
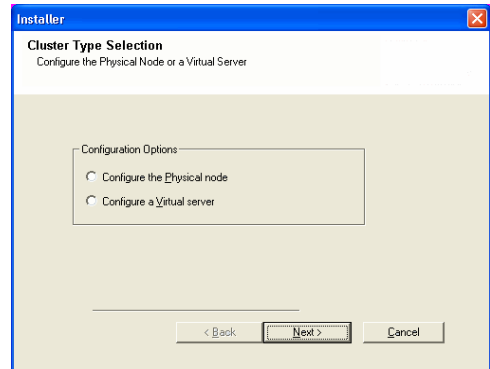
31. Select the disk group in which the cluster group resides.

Click **Next**.

32. Expand **Client Modules** | **Archive Management** and select **File Archiver for Windows Agent.**

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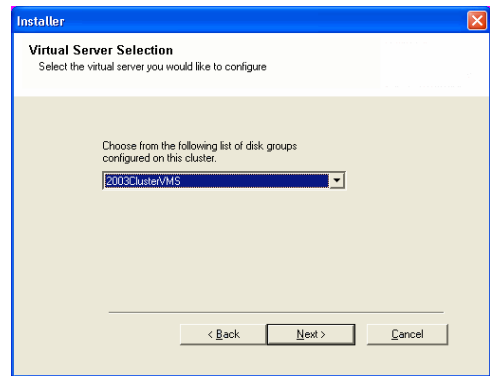
33. If this computer is separated from the CommServe by firewall(s), type **Yes** and then press **Enter**.

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

If you do not wish to configure the firewall services, type **No** and then press **Enter**.
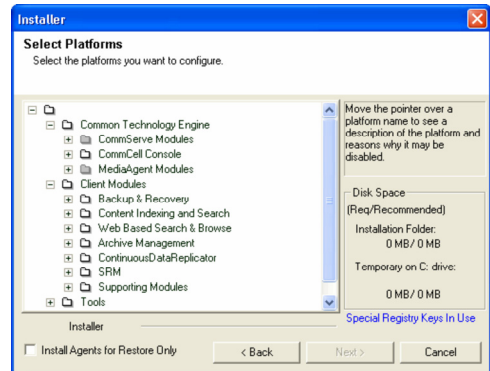
34. Enter the fully qualified domain name and Click **Next**.

- Do not use space and the following characters when specifying a new name for the CommServe Host Name:

\|`~!@#$%^&*()+=<>/?,[]{}:;'"
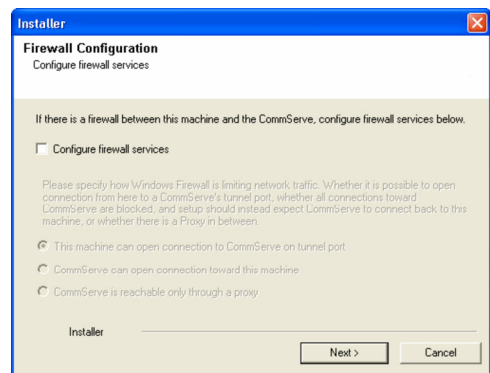
35. Click **Next**.
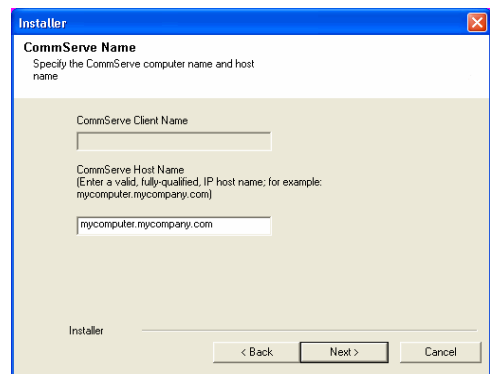
36. Select **Add programs to the Windows Firewall Exclusion List**, to add CommCell programs and services to the Windows Firewall Exclusion List.

    Click **Next**.

    > This option enables CommCell operations across Windows firewall by adding CommCell programs and services to Windows firewall exclusion list.
    >
    > It is recommended to select this option even if Windows firewall is disabled. This will allow the CommCell programs and services to function if the Windows firewall is enabled at a later time.

37. Click **Next**.

    > It is recommended to select the **Download latest update pack(s)** option to automatically install the available updates during installation.

38. Verify the default location for software installation.

    Click **Browse** to change the default location.

    Click **Next**.

    - Do not install the software to a mapped network drive.
    - Do not use the following characters when specifying the destination path:

      / : * ? " < > | #

      It is recommended that you use alphanumeric characters only.

39. Select a Client Group from the list.

    Click **Next**.

    > This screen will be displayed if Client Groups are configured in the CommCell Console.
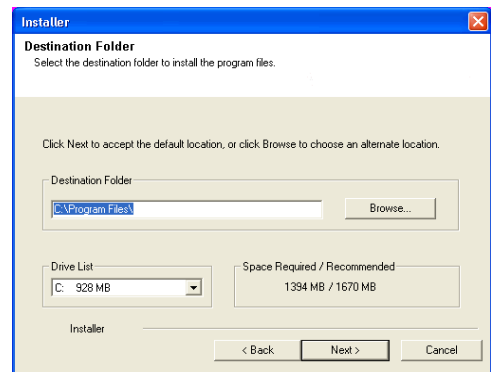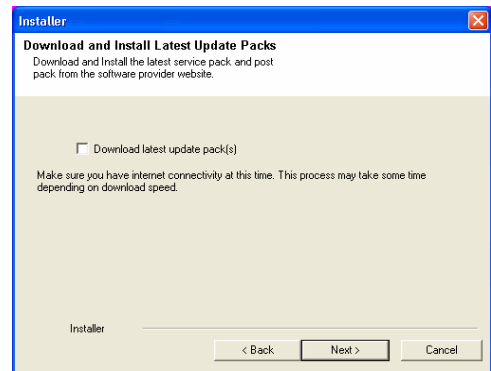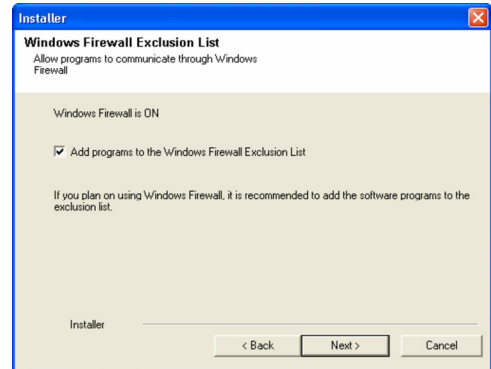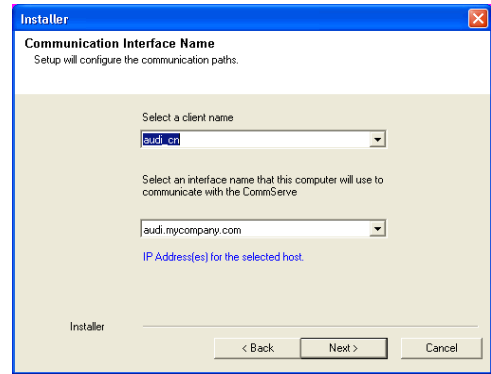
40. Click **Next**.
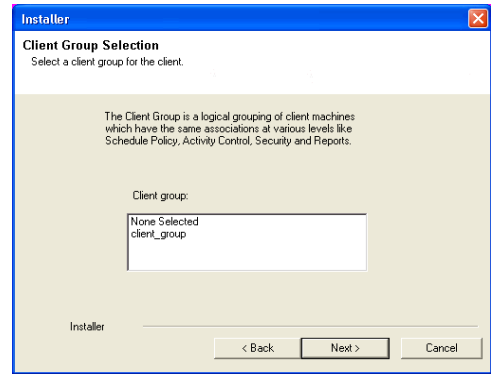
41. Click **Next**.
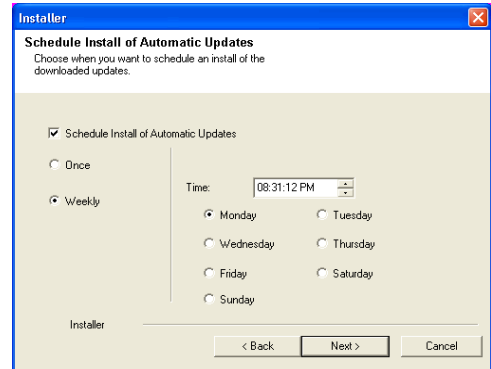
42. To install the software on the remaining nodes of the cluster, click **Yes**.

To complete the install for this node only, click **No**.
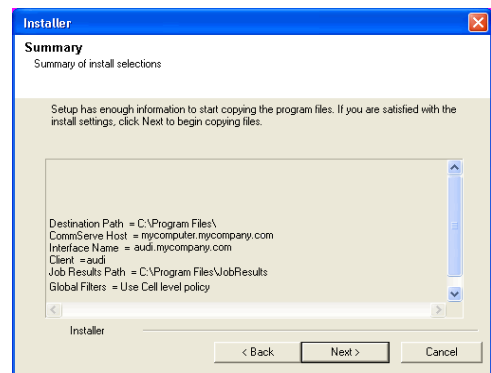
43. Select cluster nodes from the **Preferred Nodes** list and click the arrow button to move them to the **Selected Nodes** list.

Once you complete your selections, click **Next**.

- The list of **Preferred Nodes** displays all the nodes found in the cluster; from this list you should only select cluster nodes configured to host this cluster group server.
- Do not select nodes that already have multiple instances installed.
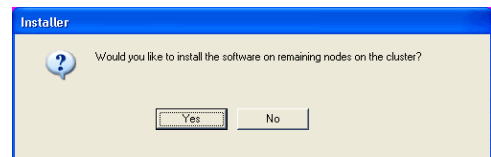
44. Specify **User Name** and **Password** for the **Domain Administrator account Information** to perform the remote install on the cluster nodes you selected in the previous step.
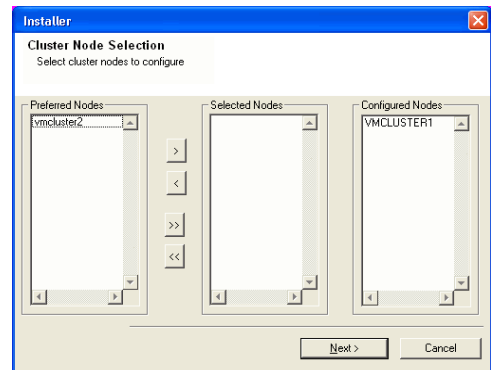
Click **Next**.

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

   ● If, during the remote install of a cluster node, setup fails to complete or is interrupted, you must perform a local install on that node. When you do, the install begins from where it left off, or from the beginning if necessary. For procedures. follow from Step 24.

46. Click **Finish**.
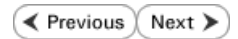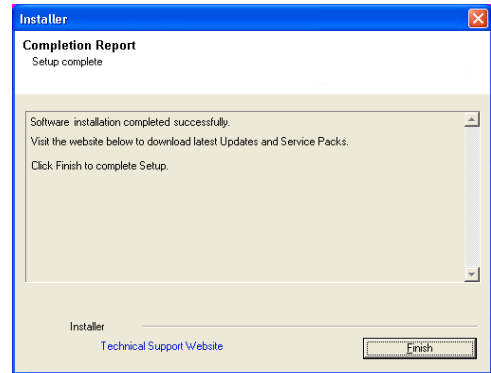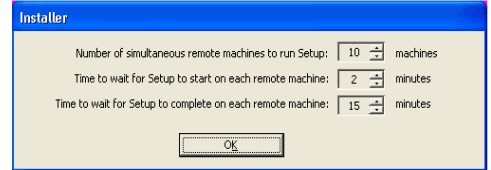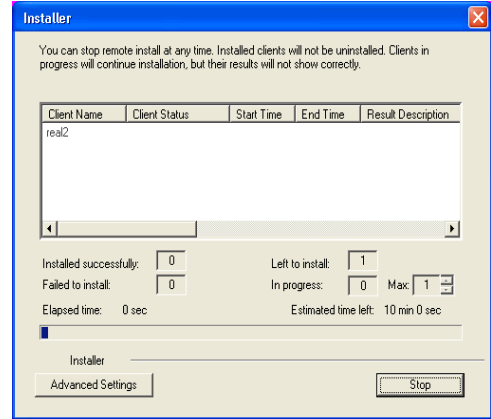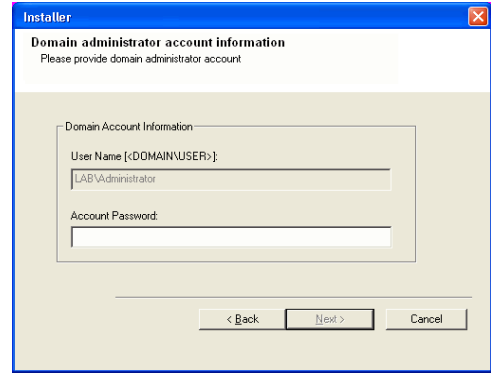
Getting Started - NetApp File Archiver Agent Configuration
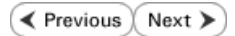
CONFIGURATION

Once the NetApp File Archiver Agent has been installed, configure an Instance and create a Subclient as follows:

1.
   - From the CommCell Browser, navigate to **<Client> | File Archiver.**
   - Right-click **File Archiver,** point to **All Tasks** | **Create Instance** and then click **FPolicy**.
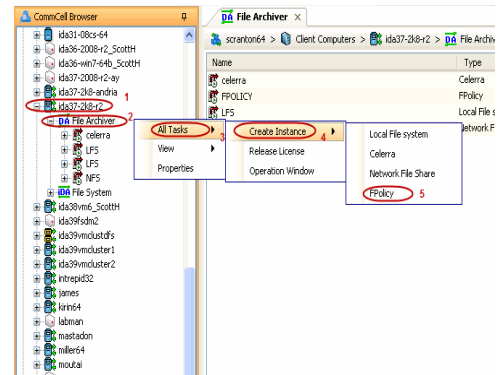
2.
   - In the **Instance Name** box enter the instance name.
   - In the **Filer Name** box enter the Filer name.

     > For Vfiler, it should use vfiler name instead of physical machine name.

   - Click **Configure Password**.
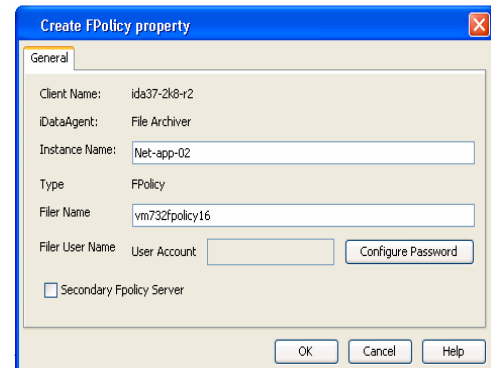
3.
   Enter credentials for an account with administrative access to the file server.

   > If you have two or more instances of NAS File Archiver configured on your CommCell Console, then use the same credentials for all instances. If you plan to use different credentials, file server must have access to those credentials.

4.
   Navigate to **<Client> | File Archiver| FPolicy Instance | DefaultArchiveSet,** point to **All Task** and select **New Subclient**.
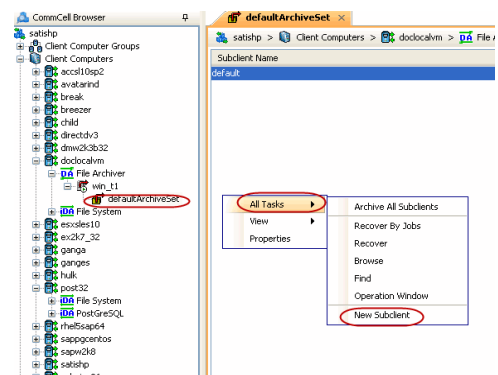
5.   In the **Subclient Name** box enter the subclient name.
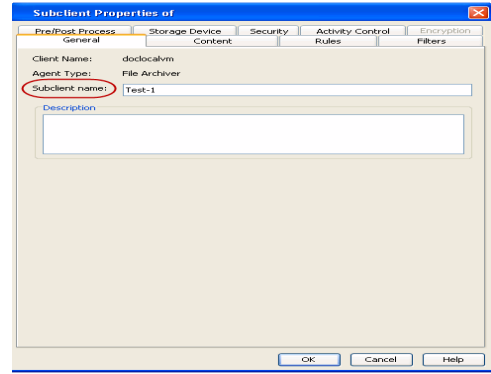
6.
- Click the **Content** tab.
- Click **Add Path** and add the path of the folders on the filer that has files to be archived.
- Click **OK**.
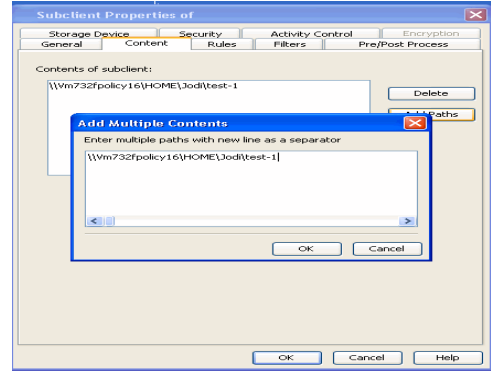
7.
- Click the **Rules** tab.
- Select **Enable All Rules**.
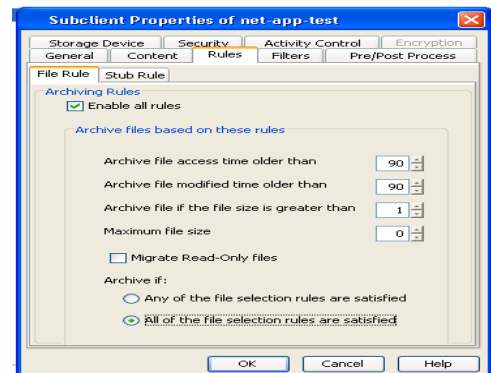
8.
- Click the **Storage Device** tab
- Select **Storage Policy**
- Click **OK**

Click **Next ▶** to continue. If you do not have Storage Policy created, click **Create Storage Policy**.
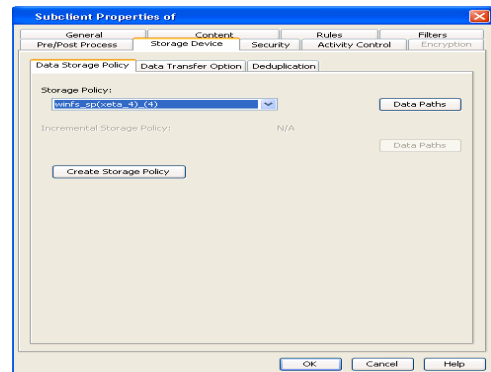
9.
1. Click **Create Storage Policy**.
2. Follow the prompts displayed in the Storage Policy Wizard. The required options are mentioned below:
   - Select the Storage Policy type as `Data Protection and Archiving`.
   - Select `No` to allow legal hold to use the policy.
   - Specify the name of the Storage Policy.
   - Specify the name of the primary copy. The primary copy is automatically created along with the Storage Policy.

○ Select <tt>No</tt> 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 <tt>Yes</tt> 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.
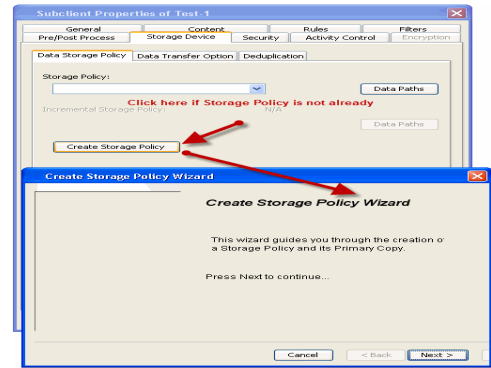
Getting Started - NetApp File Archiver Agent Migration Archiving

WHAT GETS ARCHIVED	WHAT DOES NOT GET ARCHIVED
Files on the NetApp file server	Encrypted Files
	Files with extensions `*.dll`, `*.bat`, `*.exe`, `*.cur`, `*.ico`, and `*.lnk`
	Sparse Files

PERFORM AN ARCHIVE

1.
   - From the CommCell Console, navigate to **Client Computers** | **File Archiver** | **<Instance_name>** | **defaultArchiveSet**.
   - Right-click the **Subclient** in the right-pane and click **Archive**.
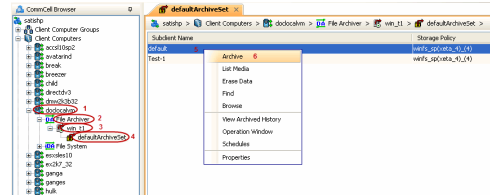
2.
   - Select **Immediate** to run the job immediately.
   - Click **OK**.
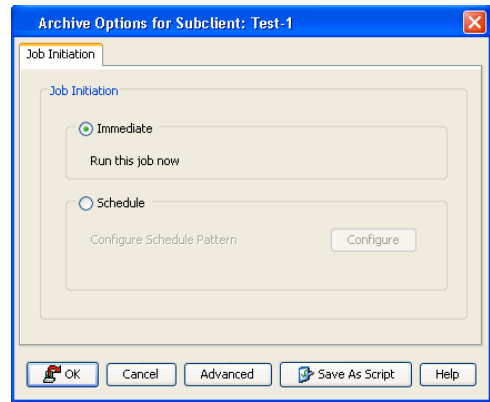
3. You can track the progress of the job from the **Job Controller** or **Event Viewer** window of the CommCell console.
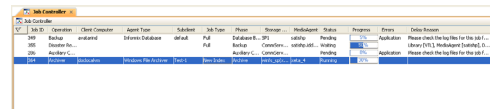
4. Once the archive process is completed, files that meet the stubbing rules are stubbed.
   - **Stubs** are placeholders of the original data after it has been migrated to the secondary storage.
   - Stubs replace the archived files in the location of the file.
   - After stubbing, the size of the files on the disk reduces.
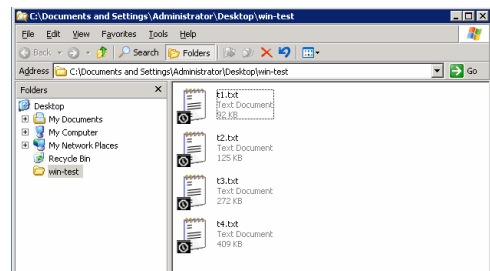
5.
   - Once job is complete, view the details of job from the **Archive Job History**. Right-click the subclient and select **View Archived History**.
   - Click **OK**.
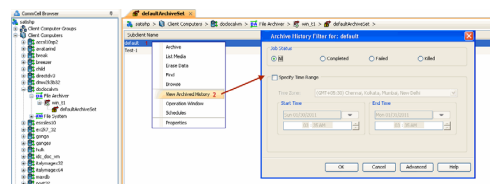
6.
   - You can view a list of the files archived during the archive job.
   - Right-click the job.
   - Click **View Stub File List**.
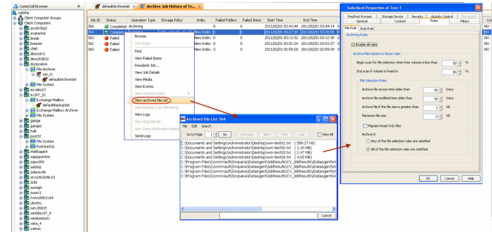
Getting Started - NetApp File Archiver Agent Recover Data

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:

1.
- Navigate to the folder with the stubs by mapping a network drive to the share or through the UNC path.
- Perform an action that executes an open and read on an archived file to initiate the recovery operation.

2.
- You can track the progress of the job from the **Job Controller** 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**.
- After recovery, stubs are replaced by files in the location specified.

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).

Advanced Configuration - File Archiver

TABLE OF CONTENTS

UNDERSTANDING THE COMMCELL CONSOLE

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

Instance - represents the type of file system that needs to be archived.

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

Subclient - defines the data to be archived.
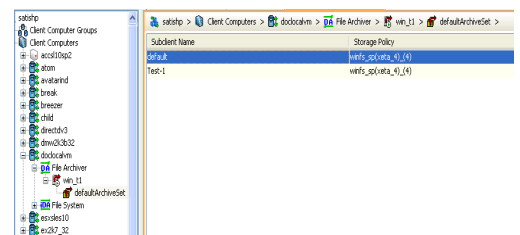
CONFIGURING RULES FOR ARCHIVING

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. The basic archving criteria is the maximum file size in a particular scanned volume/directory. Files that meet this criteria are rendered available for archiving if they satisfy any or all the archiving rules.

BASED ON 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, navigate to the **Client Computers | <Client> | File Archiver | Instance | ArchiveSet.**

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

3. Select the **Rules** tab.

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

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

6. Click **OK**.
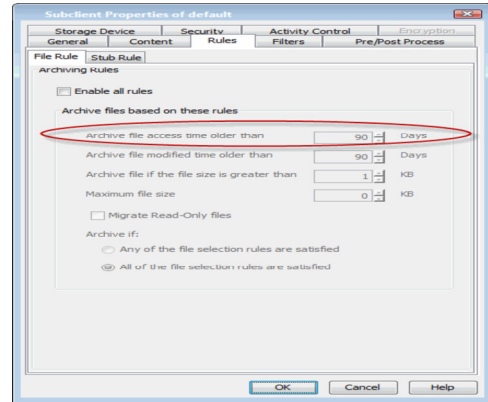
BASED ON FILE MODIFIED TIME

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, navigate to the **Client Computers | <Client> | File Archiver | Instance | ArchiveSet.**

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

3. Select the **Rules** tab.

4. Enter the number of days elapsed since the file was last modified **Archive file modified time older than *n* Days** box.

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

6. Click **OK**.
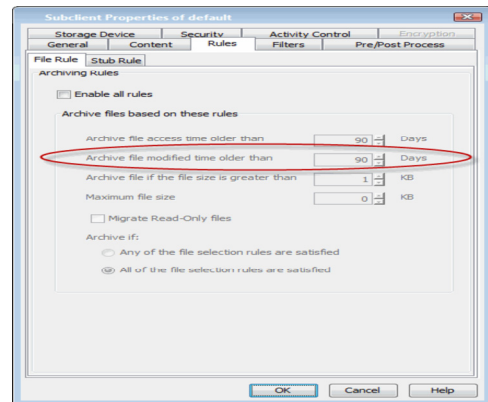
BASED ON FILE SIZE

You can also set archiving rules to archive files depending on the file size. This can be done by specifying a file size range such as files greater than 5 KB but less than 20 KB should be archived. 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, navigate to the **Client Computers | <Client> | File Archiver | Instance | ArchiveSet.**

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

3. Select the **Rules** tab.

4. Enter the minimum file size in **Archive file if size is greater than *n* KB** box.

5. Enter the maximum file size in **Maximum file size** box.

> 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**.
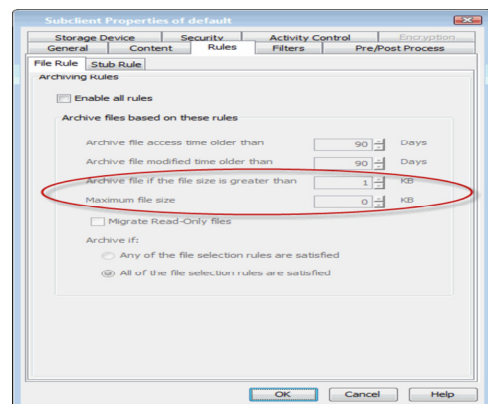
BASED ON FILE ATTRIBUTE

You can also archive the files that have the Read Only attribute set on them.

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

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

3. Select the **Rules** tab.

4. Select **Enable all Rules**.

5. Select **Migrate Read-Only Files**.

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

7. Click **OK**.
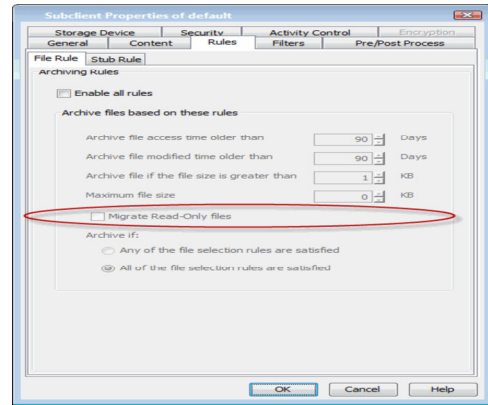
CONFIGURING POST ARCHIVING OPTIONS

REPLACING ARCHIVED FILES WITH STUBS

The configuration to delete the files after they have been archived can be modified to stub the original file after archiving. This can be done by following the steps mentioned below.

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

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

3. Select the **Rules** tab.

4. Select the **Stub Rules** tab.

5. Click **Replace File with a Stub**.

6. Click **OK**.
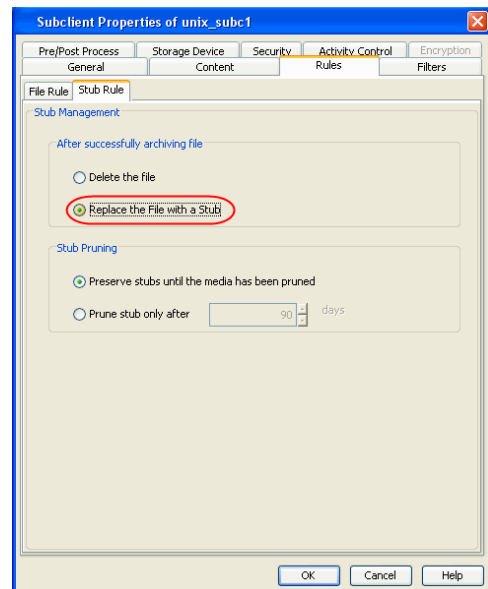
DELETING ARCHIVED FILES

You can choose to delete the files from your computer after an archiving operation in order to reclaim storage space.

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

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

3. Select the **Rules** tab.

4. Select the **Stub Rules** tab.

5. Click **Delete the File**.

6. Click **OK**.
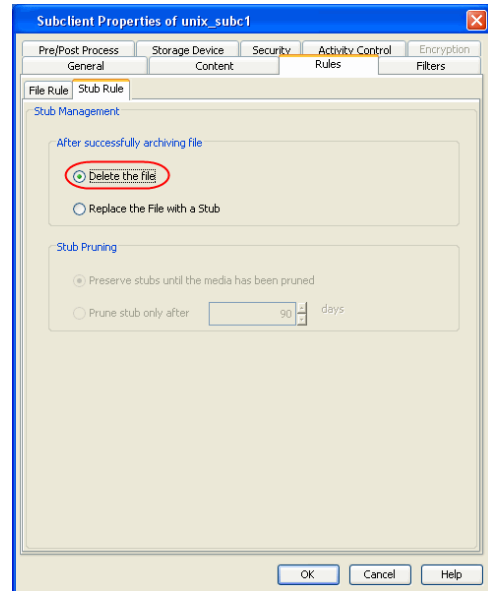
SETTING UP STUB RETENTION RULES

By default, the stubs are pruned in 90 days from the day of stubbing. However, you can set the number of days after which the stubs will be pruned by following the steps given below.

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

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

3. Select the **Rules** tab.

4. Select the **Stub Rules** tab.

5. Click **Replace File with a Stub**.

6. In the **Prune Stubs Only After <n> days** box type the number of days.

7. Click **OK**.
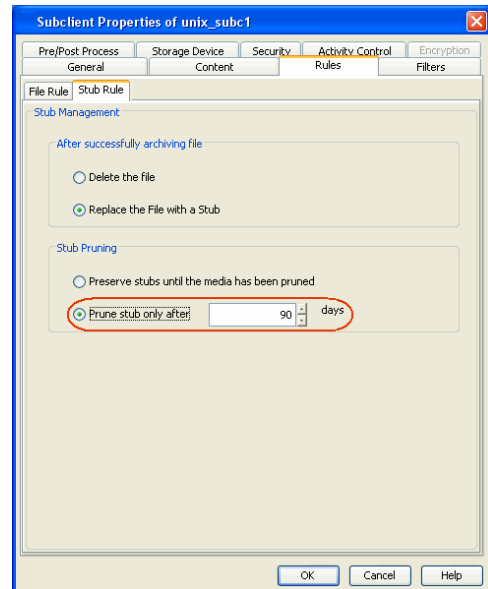
CONFIGURING A SECONDARY FPOLICY INSTANCE FOR RECALLS

You can configure a secondary FPolicy instance for recalling data in case the primary FPolicy instance is unavailable. The secondary instance for recalling data has to be configured on a client computer other than the one with the primary FPolicy instance. Once configured it will automatically take over the recalling process if the client computer with the primary instance is unavailable. Follow the steps give below to configure the FPolicy secondary instance:

1. From the CommCell Console, navigate to the **Client Computers | <Client2> | File Archiver | Instance.**

   Here **Client 1** already has a primary FPolicy Instance configured.

2. Right-click FPolicy instance and select **Properties**.

3. Select **FPolicy Secondary Server**.

4. Click **Ok**.
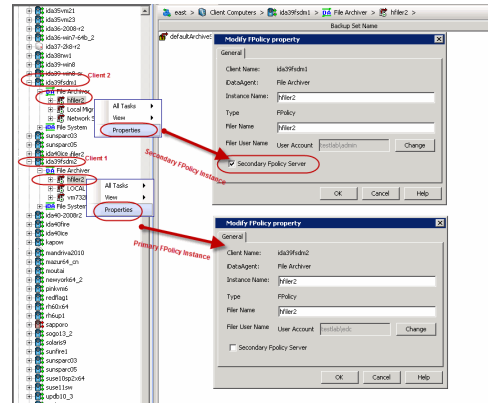
CONFIGURING FILTERS

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.

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.
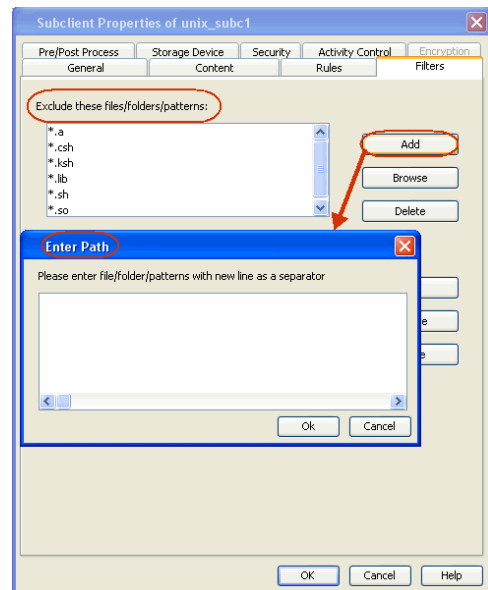
CONFIGURING EXCLUSION TO FILTERS

When excluding files from archiving, you can also provide exceptions to the data that you are excluding. For example, if you want to exclude all the files in the `My Documents` folder except the `Downloads` sub-folder, you can add a subclient filter to exclude the `My Documents` directory from being archived and also add a corresponding subclient filter to allow the `Downloads` sub-folder 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**.
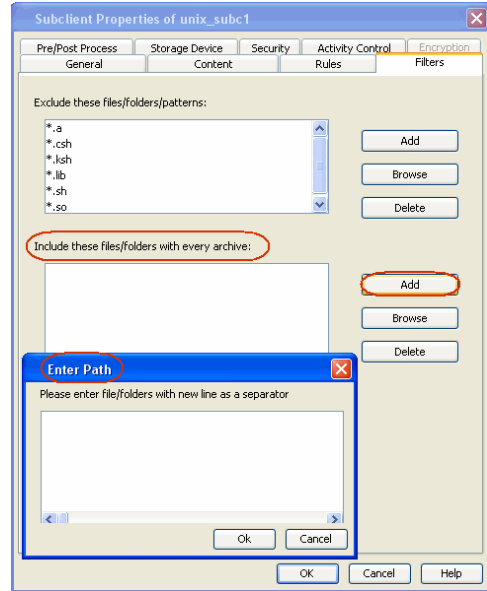
DELETING A FILTER

Filters can be deleted, when not in use. These does not included the default filters but only include the filters that were added manually. Whenever you delete a filter from the exclusion list, the system automatically deletes any exceptions that are part of the deleted exclusion filter.

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. Select the filter to be deleted and click **Delete**.

5. Click **OK**.

    It is recommended to perform a full backup after deleting the filters.
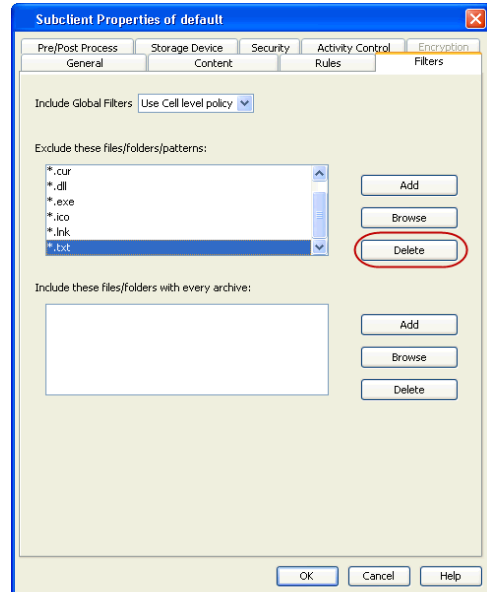
CREATING A SUBCLIENT TO BACKUP STUBS

Protecting stubs is useful for recovery operations. For example, if there is a disk failure, the data can be restored along with the stubs.

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

2. Right-click the **Backup Set** and point to **All Task**.

3. Select **New Subclient**.

4. Enter **Subclient Name** box enter the name of the subclient.

5. Click the **Storage Device** tab.

6. In the **Storage Policy** box select a Storage Policy from list.

7. Click the **Content** tab and browse to the stubs that you want to backup and click **Add**.
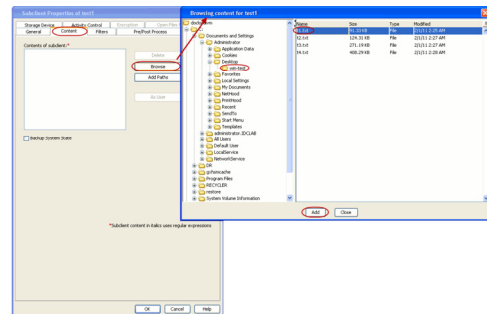
8. Click **OK**.

PROTECTING STUBS USING INCREMENTAL BACKUPS

By default the stubs are not included in Incremental Backups. Therefore stubs created after the most recent full backup may be lost if the operating system or file structure where the stubs reside is rendered unusable before the next full backup is run. Follow the steps give below to configure for stubs to be backed up during incremental backups.

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

2. Right-click the **Backup Set** and select **Properties**.

3. Click **Use Classic File Scan** and select **Check archive bit during backups** check box.

4. Click **OK**.
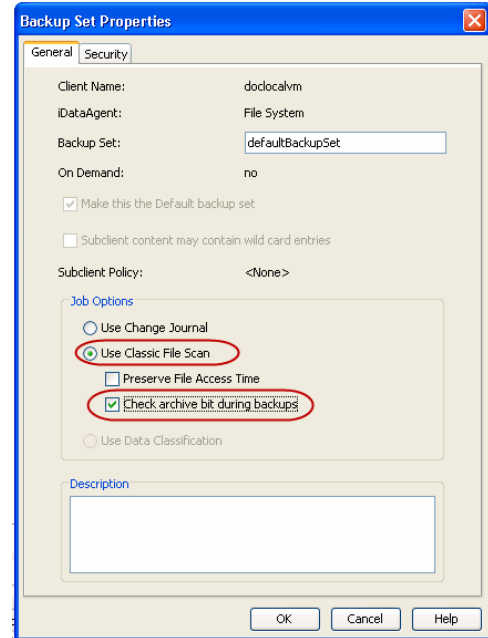
SETTING UP ON DEMAND ARCHIVING

On Demand archiving allows for content to be specified as an external input at the time of initiating an archiving operation. Whereas traditional archiving is performed using subclients, which contain fixed content configured prior to performing the operation. On Demand Archiving allows you to specify content each time you perform an archive job.

Content for On Demand Archiving is defined through:

● a **Content File**, which is a text file that defines the location of the data that you want to protect. Each Content File contains the fully qualified paths from the root directory to files, links, and devices to be archived.

Once these entities are defined, an On Demand Archive Set is then created. Archives run from this Archive Set will provide the facility to select the Content Files to be included.

CREATING CONTENT FILE

Content File entries should be in the following format with no filters, wildcards, regular expressions or paths to the FAT partition:

```
c:\data\datafile.txt
c:\data\wordfile.doc
d:\my documents\webdoc.html
```

CREATING ON DEMAND ARCHIVE SET

Create one ore more Content Files defining the content to be backed up.

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

2. Right-click **File Archiver**, point to **All Tasks** and then click **New On Demand Archive Set**.

3. In the **New Archive Set Name** box, type a name (up to 32 characters).

4. In the **Storage Policy** box select a storage policy.

5. Click **OK**

Once an On Demand Archive Set has been created, it cannot

be changed into a traditional archive set.
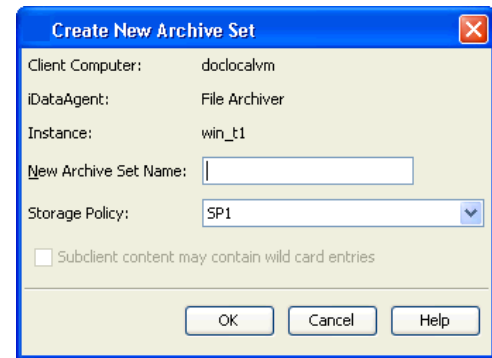
ADDING FILES AND FOLDERS WITH UNICODE CHARACTERS TO CONTENT FILES

If the path or the filename contains Unicode characters, the Content File must be converted to a format that can be used by the data protection operation. The Unicode Conversion utility must be used to convert the Content File to a format that can be provided as input.

1. Using a text editor, create a file that contains a list of files/folders with Unicode characters. Make sure to save the file as a Unicode text file.

2. From the Command Line, navigate to the `<software install folder>/base` folder and type the following:

   cvconvertunicode <source file> <destination file>

   Where:

   <source file> is the full path and name of the file created in Step 1.

   <destination file> is the full path and name of the destination file. The file will automatically be created by the utility.

3. Use the destination file as the content file to perform an On-Demand archive.

PREVENTING DUPLICATES

On Demand Archive explicitly archives the files listed in the Content File. If the Content File contains two entries for a file, the file will be backed up twice.

For example:

```
c:\data
```

```
c:\data\files
```

In this scenario, an archiving operation will archive the contents of all data residing in the `files` folder twice as the Content File has already called for the entirety of the parent folder to be archived. It is recommended that Content Files not include such duplicate entries.

However, if it is not feasible to monitor a Content File for such duplicate entries, the `OnDemand_AutoExpandDir` registry key can be created on the computer in which the Content File is located. This key prevents the scan phase of an archive job from expanding through all subfolders within a path listed in the Content File.

In the case of the above example, only the root contents of the files will be included in the archiving operation. The subfolders will not be included to prevent duplicate data.

To create this key, perform the following steps:

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

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

3. Select **Properties**.

4. Select the **Registry Key Settings** tab**.**

5. Click **Add**.

6. In the **Name** box enter `FileSystemAgent`.

7. In the **Location** box enter `HKEY_LOCAL_MACHINE\SOFTWARE\CommVault Systems\Galaxy\Instance<xxx>\`.

8. In the **Type** box select DWORD.

9. In the **Value** box enter `OnDemand_AutoExpandDir`.

10. Click **OK**.
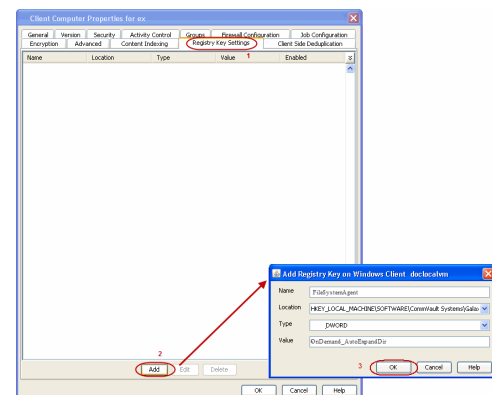
CONFIGURING THE MAXIMUM NUMBER OF SIMULTANEOUS STUB RECALLS (RECALL THROTTLING)

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.
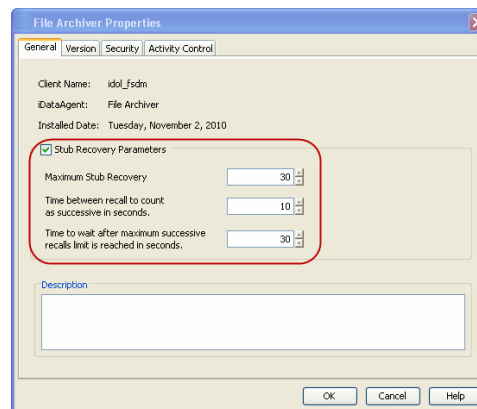
EXAMPLES OF RECALL THROTTLING

For the examples below, we will assume that the recovery administrator has established the following recall throttling parameters:

● Maximum Stub Recovery (i.e., limit) is set to 10.

● Time Between Recall to Count as Successive in Seconds (i.e., interval) is set to 30 seconds.\

● Time to Wait after Maximum Successive Recalls Limit is Reached in Seconds (i.e., cool-down) is set to 60 seconds.

EXAMPLE DESCRIPTION	USER ACTION	RESULT
Maximum Limit is Not Exceeded (with no additional recall requests).	A user submits 4 stub recovery requests at the same time on a given client, and no other stub recovery requests are submitted on that client during the 30 second interval that follows.	As each stub recovery request is received, it will begin processing immediately and the 30 second interval countdown will begin where the system will wait to see if any more stub recovery requests are submitted. There is no cool-down period since the limit was not reached, and all 4 files will be recovered.
Maximum Limit is Exceeded (with no additional recall requests).	A user submits 20 stub recovery requests at the same time on a given client, and no other stub recovery requests are submitted on that client during the 30 second interval that follows.	The first 9 stub recoveries will begin immediately, the 30 second waiting interval does not apply here since the limit has been reached, and the 60 second cool-down period begins where no other stub recovery requests will be accepted. 11 stub recovery requests (out of 20) that were over the limit will not be processed, and an event will be issued in the CommCell Console's Event Viewer and the Windows Event Viewer indicating that the limit has been reached. The first 9 files will be recovered, and depending on the agent the user will see one of the following results for the 11 stub recovery requests that were over the limit. Assuming they were text files, 11 blank Notepad sessions appear on the desktop.
Maximum Limit is Not Exceeded (with additional recall requests received within the Interval).	A user submits 4 stub recovery requests at the same time on a given client, and 4 other stub recovery requests are submitted on that client by another user during the 30 second interval that follows.	As each stub recovery request is received from the user, it will begin processing immediately and the 30 second interval countdown will begin where the system will wait to see if any more stub recovery requests are submitted. After 20 seconds have elapsed, the 4 additional stub recovery requests are received so the 30 second interval countdown will begin again (i.e., the count is initialized to zero) to allow one more request to be submitted. Since the limit has not been reached, the cool-down period does not apply, and all 8 files will be recovered on a first-in first-out basis.
Maximum Limit is Not Exceeded (with additional recall requests received outside the Interval).	A user submits 4 stub recovery requests at the same time on a given client, and 8 additional stub recovery requests are submitted on that client by another user 35 seconds later.	As each stub recovery request is received from the user, it will begin processing immediately and the 30 second interval countdown will begin where the system will wait to see if any more stub recovery requests are submitted. After 35 seconds have elapsed, 8 additional stub recovery requests are received and the 30 second interval countdown will begin again (i.e., the count is initialized to zero) to allow one more request to be submitted. Since the limit was never reached during the first or second interval, the cool-down period does not apply, and all 12 files will be recovered on a first-in first-out basis.

CONFIGURING FOR NETAPP FILE SERVERS ON ONTAP 7.0

In order to be able to archive and restore data for NetApp file servers running on ONTAP 7.0 ensure that the following are configured:

● The fully qualified domain name is specified in the instance properties and also the subclient content path.

● GXHSM_FPOLICY_EXCLUDE_NON_GENERIC and GXHSM_FPOLICY_SCREEN_FS_OP_CREATE keys have been created in the computer where NetApp File Archiver Agent is installed.

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

2. Right-click the **Client.**

3. Select **Properties.**

4. Select the **Registry Key Settings** tab**.**

5. Click **Add**.

6. In the **Name** box enter GXHSM_FPOLICY_EXCLUDE_NON_GENERIC.

7. In the **Location** box enter WinFSDataMigrator.

8. In the **Type** box select Reg_SZ.

9. In the **Value** box enter **N**

10. Click **OK**.

11. Click **Add**.

12. In the **Name** box enter GXHSM_FPOLICY_SCREEN_FS_OP_CREATE.

13. In the **Location** box enter WinFSDataMigrator.

14. In the **Type** box select Reg_SZ.

15. In the **Value** box enter **Y**

16. Click **OK**.

17. Restart the Data Archiver services.
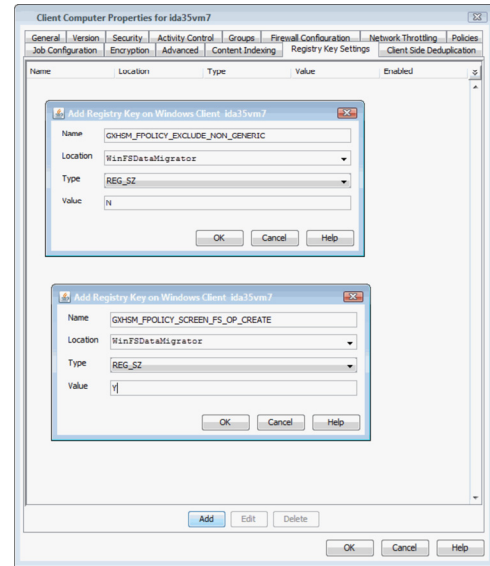
CONFIGURING FOR RESTUBBING

By default when a stub is recalled but no changes are made to its content, it is re-stubbed during the next archiving cycle. During restubbing, the stubs are replaced by the existing copies of the stub available in the stub cache. However for Windows 2008 the following registry key should be created in the computer with NetApp File Archiver agent installed for successful restubbing.

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

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

3. Select **Properties.**

4. Select the **Registry Key Settings** tab**.**

5. Click **Add**.

6. In the **Name** box enter GXHSM_FPOLICY_REGISTER_FILERNAME.

7. In the **Location** box enter iDataAgent.

8. In the **Type** box select Reg_SZ.

9. In the **Value** box enter **<xyz>**

   Where **xyz** is the Filer Name

10. Click **OK**.
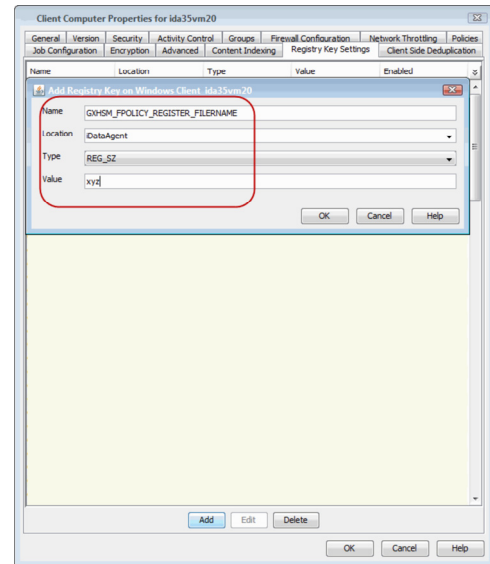
MODIFYING AN ARCHIVE SET, INSTANCE OR SUBCLIENT

The following table describes the properties that can configured from the agent, instance, 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.**	Refer to Activity Control.

	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.**	
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 Instance	You can rename an existing Instance. 1. From the CommCell Browser, right-click the Instance. 2. Click **Properties.** 3. Click **General** tab and type the new name in the Instance field. 4. Click **OK** to save your settings.	
Rename Archive Set	You can rename an existing Archive Set. 1. From the CommCell Browser, right-click the Archive Set. 2. Click **Properties.** 3. Click **General** tab and type the new name in the Archive 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.
	
	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.
		Refer to Pre/Post Processes.

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. 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**.	Refer to User Administration and Security.
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. 1. From the CommCell browser, right-click the subclient. 2. Click **Properties.** 3. Click **Encryption.** 4. Select the desired encryption. 5. Click **OK**.	Refer to Data Encryption.
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. 1. From the CommCell browser, click **Reports** icon. 2. Select **CommCell Configuration**. 3. Click **Run**.	Refer to CommCell Configuration.

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.	Refer to Archive/Compliance Archive Job Summary Report
	1. From the CommCell browser, click **Reports** icon.	
	2. Select **Job Summary**.	
	3. Click **General** and select **Archive/Compliance Archive.**	
	4. Click **Run**.	

MODIFYING A CLIENT, INSTANCE OR SUBCLIENT FROM THE COMMAND LINE

MODIFYING A CLIENT

The GXHSMUtility provides additional options that can be set on the client. These options can be set from the command line and are not available from the Client Properties dialog in the CommCell Console.

1. Access the command prompt on the computer, where File Archiver Agent is installed.

2. Navigate to the <File Archiver Agent >\Base> folder

3. Run the GXHSMUtility utility.

Usage: The following table lists the command line options and their description.

OPTION	DESCRIPTION
RestubOn [x]	Enables restub logic in the recall phase
RestubOff	Disables restub logic in the recall phase
OffLineAtOn [x]	Enable setting offline attribute for NAS sub clients
OffLineAOff	Disable setting offline attribute for NAS sub clients
CheckAlwaysOn	Enable recall logic to ALWAYS check sub client recall property
SetExtPropStr	Set the extended property name.
GetExtPropStr	Retrieve the extended property name.
SetExtPropNum	Set the extended property number.
GetExtPropNum	Retrieve the extended property number.
CheckAlwaysOff [x]	Disable recall logic to check sub client recall property

MODIFYING AN INSTANCE

You can use the GXHSMutility to set additional options on the instance from the command line.

1. Access the command prompt on the computer, where File Archiver Agent is installed.

2. Navigate to the <File Archiver Agent >\Base> folder

3. Run the GXHSMUtility utility.

Usage:

OPTION	DESCRIPTION
SetExtPropStr	Set the extended property name.
GetExtPropStr	Retrieve the extended property name.
SetExtPropNum	Set the extended property number.
GetExtPropNum	Retrieve the extended property number.

MODIFYING A SUBCLIENT

You can use the GXHSMUtility to set additional options on subclients. These options are not available from the subclient properties dialog box in the CommCell Console. When using these additional options, make sure to specify the subclient name along with the setting. If the subclient name is not specified, the setting is applied to all the subclients.

Usage:

OPTION	DESCRIPTION
SysHid	Enables sub-client to migrate system and hidden files
SysHidOff	Disallow migration of system or hidden files
ModCreate	Maintain file modification and creation time on migration
AccessTimeM	Maintain file access time on migration [requires ModCreate]

AccTimeMOff	Disables access time preservation during migration
AccessTimeR	Maintain file access time on recall [requires ModCreate]
AccTimeROff	Disables access time preservation during recall
KeepTimeOff	Disables ALL time preservation during migration
SparseOn	Enable sparse; Enabled by default for local; For fpolicy, this option is only supported on OnTap 7.3 & higher, and it's enabled by default for supported versions
SparseOff	Disable sparse
RestubOn	Enables restub logic on migration per subclient
RestubOff	Disables restub logic on migration per subclient. Client level RestubOff needs to be used with subclient level restub options. The client level restub option is used in the recall phase, and applies to all sub-clients.
IgnreSparse	Ignore sparse attribute when migrating files; This is commonly used for fpolicy.
IgnrSprsOff	Turn off IgnreSparse option
DontStubOn	Do not stub file in stub phase, and do not delete; Only archive
nDontStubOff	Turn off DontStubOn option
NasSparse	When recalling NAS files, remove sparse
NasSprsOff	Turn off NasSparse option
DisableAcls	Disables restoring ACLs during recall
EnableAcls	Turn off DisableAcls option
StageRecall	Enable recalls to use staging folder (gxhsmcache)
StageOff	Disables StageRecall
RmtErrMsg	Remote error message handling on. When this is set, a popup message is sent to remote users when recall error occurs.
SetExtPropStr	Set the extended property name.
GetExtPropStr	Retrieve the extended property name.
SetExtPropNum	Set the extended property number.
GetExtPropNum	Retrieve the extended property number.
RmtErrMsgOf	Disables RmtErrMsg

DELETING AN AGENT, INSTANCE, ARCHIVE SET 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.

DECONFIGURING AN INSTANCE

Consider the following before deconfiguring an instance:

- The Instance will appear dimmed or greyed-out in the CommCell Browser. Functionality related to issuing an archive job will not be available. However, browse and restore operations are available.

- The related files and registry entries associated with the Instances will not be removed from the computer. For example, the subclients associated with the Instance will be hidden and can be re-displayed if the instance is reconfigured with the **Reconfigure** option.

- To permanently delete all data and job history, delete the Instance in the CommCell Console.

- The license is released if the Instance that is being deconfigured is the last instance to use that license. The license is re-enabled when a new Instance is created or if the Instance is reconfigured with the **Reconfigure** option.

- All Data Archive/Data Recovery job schedules (independent and those part of a schedule policy), which are related to the specific Instance will continued to be displayed in the Schedule Details dialog box after the Instance has been deconfigured.

1. From the CommCell Browser, navigate to the instance that you want to deconfigure.

2. Right-click the instance, click **All Tasks** and then click **Deconfigure.**

DELETING AN INSTANCE

Consider the following before deleting an instance:

● When you delete a specific instance all job schedules and job histories that pertain to any of the levels within the deleted instance are deleted.

● You cannot delete an instance if it is being backed up. Attempts to delete an instance under such conditions cause the deletion to fail. If a backup is in progress, either wait for the backup to complete or kill the backup job using the Job Manager. Once the backup is no longer in progress, you can delete the instance level.

● You cannot delete an instance if there is only one instance present for an agent. To delete the final instance, you must remove the agent software from the client computer.

1. From the CommCell Browser, right-click the instance that you want to delete, click **All Tasks** and then click **Delete**.

2. Click **Yes** to confirm the deletion. (Clicking **No** cancels the deletion and retains the node.)

3. Type the requested phrase in the **Enter Confirmation Text** dialog box and click **OK**. This should delete the instance.

DELETING AN ARCHIVE SET

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 - NetApp File Archiver

TABLE OF CONTENTS

SCHEDULING AN ARCHIVE JOB

1.
- From the CommCell Console, navigate to **Client Computers** | **File Archiver** | **<instance_name>** | **defaultArchiveSet.**
- In the right pane right-click the **Subclient** 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.
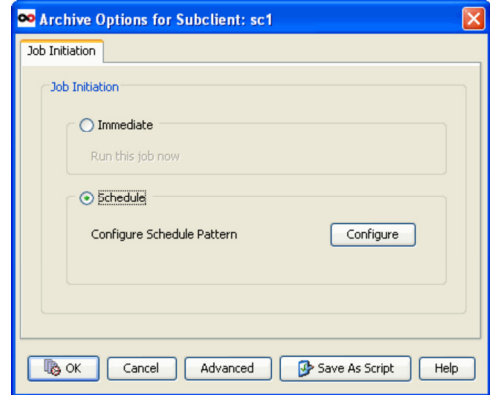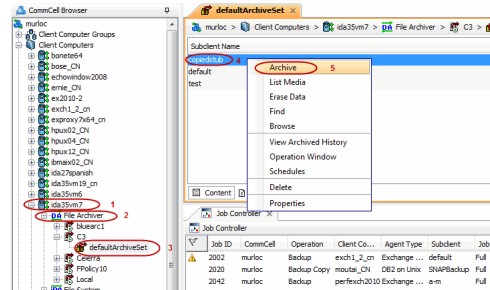
3. In the **Schedule Details** dialog box select the appropriate scheduling options.

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.
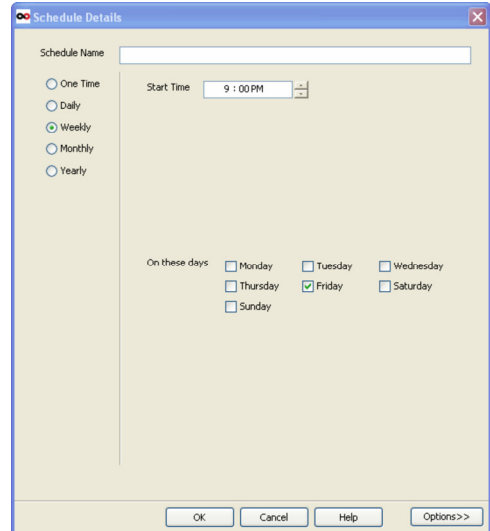
RUNNING A BACKUP TO PROTECT STUBS

The stubs of the archived data can be protected by running a full backup. In case the data has both Windows and Unix ACLs then it is recommended to use NAS

NDMP *i*DataAgent for backing up the stubs .Follow the steps given below:

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

2. In the right pane right-click the new **Subclient** and click **Backup**.

3. Select **Full** as backup type and **Immediate** to run the job immediately.

4. Click **OK**.

5. You can track the progress of the job from the **Job Controller** window of the CommCell console.

6. Once job is complete, view the details of job from the **Backup History**.

7. Right-click the **Subclient** and select **Backup History**.

8. Click **OK**.
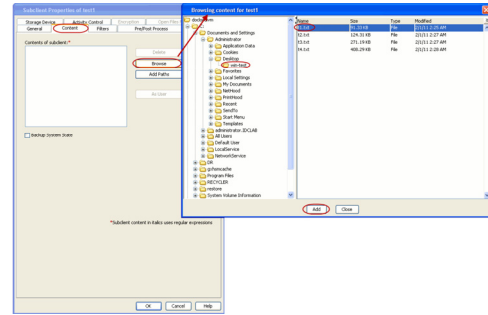
SCHEDULING STUB BACKUPS

An incremental backup contains only data that is new or has changed since the last backup, regardless of the type. Therefore the stubs that are created after the full backup can be protected by running an incremental backup. On an average, incremental backups consume far less media and uses less resources than full backups.

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

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

3. Select **Incremental** as backup type and **Immediate** to run the job immediately.

4. Click **OK**.

   You can track the progress of the job from the **Job Controller**. When the backup has completed, the **Job Controller** displays **Completed**.
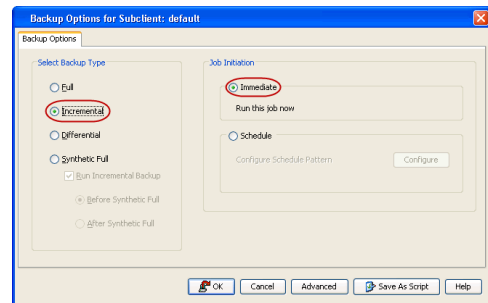
MANAGING JOBS

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.
   - 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.**
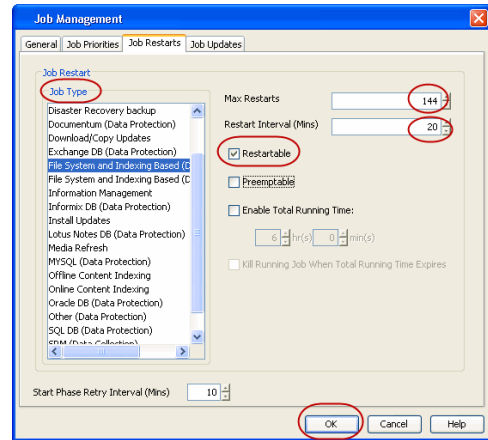
CONFIGURE JOB RESTARTABILITY FOR AN INDIVIDUAL JOB

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.**
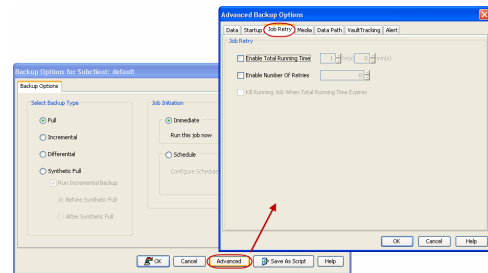
CONTROLLING JOBS

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.

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 archive data options for the archive operation.	

	1. From the CommCell Browser, click **Client Computers| <client> | File Archiver | Instance | ArchiveSet**. The default and other subclients (if available) are displayed on the right-hand window pane. 2. Right-click the subclient in the right-pane 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 archive data options for the archive operation. 1. From the CommCell Browser, click **Client Computers |<client> | File Archiver | Instance | ArchiveSet**. The default and other subclients (if available) are displayed on the right-hand window pane. 2. Right-click the subclient in the right-pane 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 |<client> | File Archiver | Instance | ArchiveSet**. The default and other subclients (if available) are displayed on the right-hand window pane. 2. Rght-click the subclient in the right-pane 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 | <client> | File Archiver | Instance | ArchiveSet**. The default and other subclients (if available) are displayed on the right-hand window pane.
	
	2. Right-click the subclient in the right-pane 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	Refer Change Data Path for more information.

	system automatically identifies the data path for the backup operations. 1. From the CommCell Browser, click **Client Computers | <client> | File Archiver | Instance | ArchiveSet**. The default and other subclients (if available) are displayed on the right-hand window pane. 2. Right-click the subclient in the right-pane that contains the data you want to archive. 3. Click **Archive**. 4. **Archive Options** for Subclient window, click **Advanced**. 5. 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. 6. Click **OK**.	
Vault Tracking	The VaultTracker feature provides the facility to manage media that are removed from a library and stored in offsite locations. 1. From the CommCell Browser, click **Client Computers | <client> | File Archiver | Instance | ArchiveSet**. The default and other subclients (if available) are displayed on the right-hand window pane. 2. Right-click the subclient in the right-pane that contains the data you want to archive. 3. Click **Archive**. 4. ght-click the Subclient and select **Archive**. 5. From the **Archive Options for Subclient** window, click **Advanced**. 6. From the **VaultTracking** tab, select the necessary options. 7. 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. From the CommCell Browser, click **Client Computers | <client> | File Archiver | Instance | ArchiveSet**. The default and other subclients (if available) are displayed on the right-hand window pane. 2. Right-click the subclient in the right-pane that contains the data you want to archive. 3. Click **Archive**. 4. Click **Advanced**. 5. On the **Alert** tab, click **Add Alert** and it opens **Add Alert Wizard** window. 6. From the **Add Alert Wizard** window, select the **Threshold and Notification Criteria**. Click **Next**. 7. Select the **Notification Types**. Click **Next**. 8. Select the **Users and User Groups**. Click **Next**. 9. Click **Finish**.	Refer Alerts for more information.

Advanced Recovery - NetApp File Archiver

TABLE OF CONTENTS

STUB RECOVERY OPTIONS

COPYING STUBS WITHOUT TRIGERRING A RECALL

When stubs are copied across drives or on mount points on the same drive it may trigger a stub recall. When copying stubs, UNC paths must be provided for FPolicy stubs. To copy stubs from one location to another without triggering a recall, follow the steps given below:

1. Access the command prompt on the computer, where NetApp File Archiver is installed.

2. Navigate to the <File Archiver NetApp >\Base> folder

3. Run the GXHSMUtility utility.

    Usage: GXHSMUtility [-stubonly] <file_src> <file_dest>

RECOVER DATA USING COMMCELL CONSOLE

RESTORING DATA

Use the following method to recover data and 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 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 **Recover to Same Paths** box or in the **Specify destination path** box type the destination path or click **Browse** to locate the desired destination.

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

8. Select **Immediate**.

9. Click **OK**.

10. You can monitor the progress of the restore job in the **Job Controller** 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.
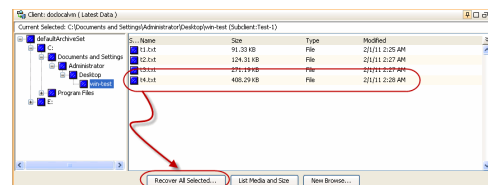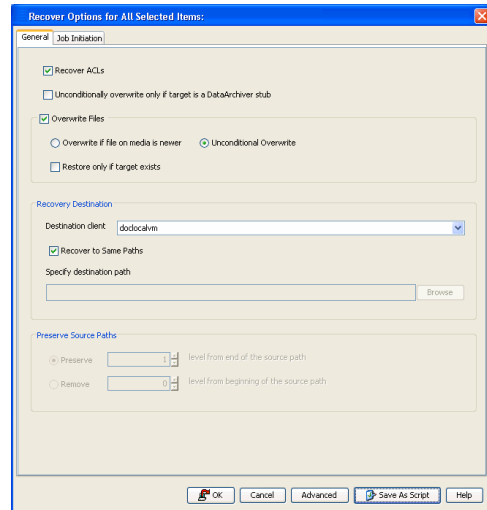
PERFORMING A DIRECT RESTORE

Perform a direct restore in the following scenarios:

- You know the path to the data that you want to restore
- The data that you want to restore is from a single volume

If you want to restore data from multiple volumes, perform a browse and restore.

Follow the steps given below to perform a direct restore:

1.
- From the CommCell Browser, navigate to **Client Computers | <Client> | File Archiver | Instance**.
- Right-click the **defaultArchiveSet** and then click **All Tasks | Restore**.

2. Enter the starting path of the data that you want to restore.

3.
- Select the name of the client computer from the **Destination Client** list.
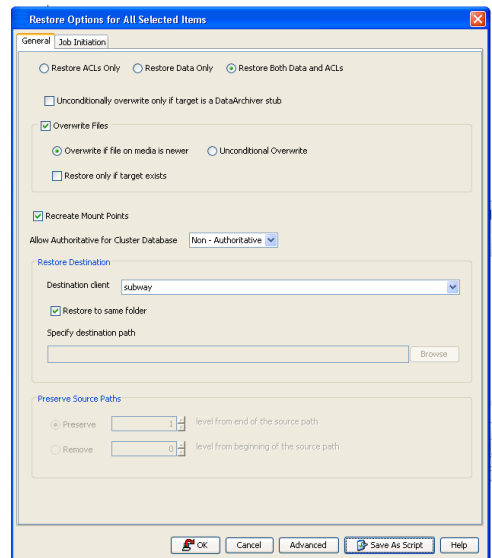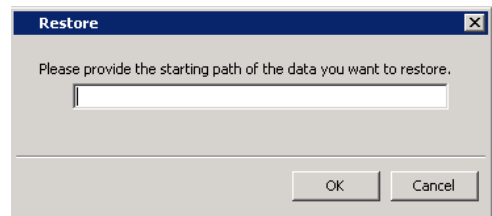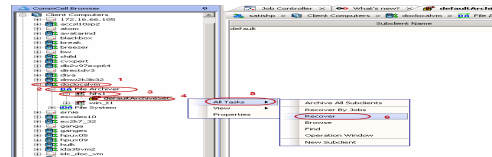
4.
- Select **Immediate** from the **Job Initiation** tab.
- Click **OK**.
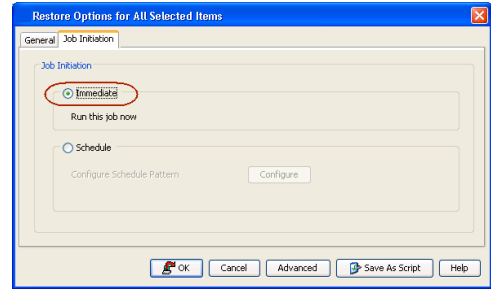
5. You can track the progress of the job from the **Job Controller**.

PERFORMING AN OUT-OF-PLACE RESTORE

You can restore the data to following locations:

- Different folder on the same computer from which the data is archived
- Different computer

Keep in mind that the destination computer must reside in the same CommCell as the client whose data was archived.

RESTORING TO DIFFERENT FOLDER ON THE SAME CLIENT

Follow the steps given below to restore data to a different folder on the same client from which data is archived:

1. From the CommCell Browser, navigate to **Client Computers | <*Client*> | File Archiver | Instance |<Archive Set>** .
2. Right-click the subclient in the right pane and then click **Browse**.
3. Click **OK**.
4. Select data that you want to restore and click **Recover All Selected**.
5. Clear the **Recover to same folder** check box and click **Browse**.
6. Select the destination folder and click **OK**.
7. Select one of the following options:
   - **Preserve <n> level from end of source path** - Select this option and enter the number of levels. The specified levels of folders from the end of source path will be restored in the destination folder.

     For Example: If the selected data is `Documents\Memos\Sales`, this option is set to 1 and the Destination folder is `temp`, the data will be restored as `\temp\Sales`.
   - **Remove <n> level from beginning of source path** - Select this option and enter the number of levels. The specified levels of folders from the beginning of the source path will not be restored.

     For Example: If the selected data is `Documents\Memos\Sales`, this option is set to 1 and the Destination folder is `temp`, the data will be restored as `\temp\Memos\Sales`.
8. Click **OK.**
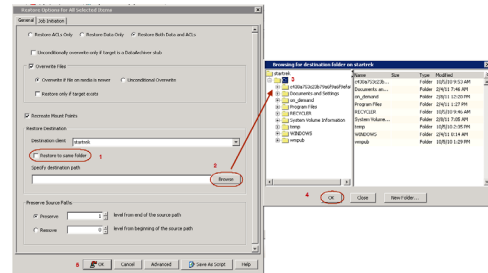
RESTORING DATA TO A DIFFERENT CLIENT

Follow the steps given below to restore data to a different client:

1. From the CommCell Browser, navigate to **Client Computers | <*Client*> | File Archiver | Instance |<Archive Set>** .
2. Right-click the subclient in the right pane and then click **Browse**.
3. Click **OK**.
4. Select data that you want to restore and click **Recover All Selected**.
5. Select the **Destination Client**. You can select any client that is in the same CommCell as that of the client from which the data was archived.
6. Click **OK**.

   If you don not clear **Restore to same folder** check box, the data will be restored to the same folder on the destination client. All the existing data in that folder will be overwritten during the restore operation.
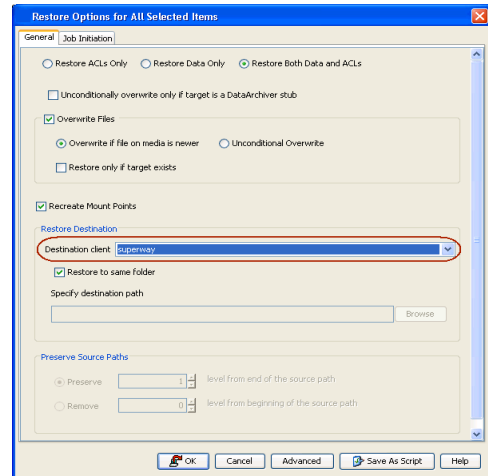
PERFORMING A CROSS-PLATFORM RESTORE

You can perform the following cross-platform restores :

- Restores across all the supported versions of Windows.

- Restores from Windows to all the supported versions of Unix.

Follow the steps given below to perform a cross-platform restore:

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

2. Right-click the subclient in the right pane and then click **Browse**.

3. Click **OK**.

4. Select data that you want to restore and click **Recover All Selected**.

5. Select the **Destination Client**. You can select any client that is in the same CommCell as that of the client from which the data was backed up.

6. Clear the **Restore to same folder** check box and click **Browse**.

7. In the **Browsing for destination folder on <client>** dialog box, select the destination folder and click **OK**.

8. In the **Restore Options for All Selected Items** dialog box, click **OK**.

> When you are restoring to a Windows client, you can also select the **Restore to same folder** check box. The existing data in that folder may get overwritten during the restore operation.
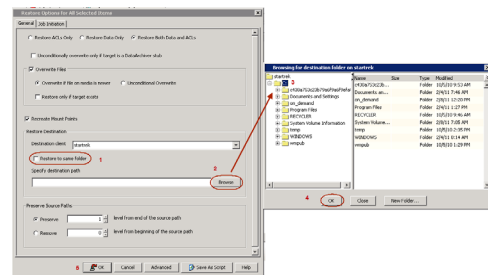
RESTORE TO A UNC PATH/NFS-MOUNTED FILE SYSTEM

Follow the steps given below to restore data to a UNC path (Windows) or NFS-mounted file system (Unix).

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

2. Right-click the subclient in the right pane and then click **Browse**.

3. Click **OK**.

4. Select data that you want to restore and click **Recover All Selected**.

5. Select the computer that hosts the share or mounted file system as the **Destination Client** .

6. Clear the **Restore to same folder** check box and enter the UNC path or the network share.

   For example: \\servername\sharename\directory

7. When you are restoring to a UNC path (Windows), click the **Advanced**.

8. From the **General** tab of the **Advanced Restore Options** dialog box, select the **Impersonate User** option.

9. Enter a username and password that has all permissions for the folder to which the data will be restored. This user should be allowed to create files in the in the destination folder of the client where you are restoring the data.

10. In the **Advanced Restore Options** dialog box, click **OK**.

11. Click **OK** in the **Restore Options for All Selected Items** dialog box.
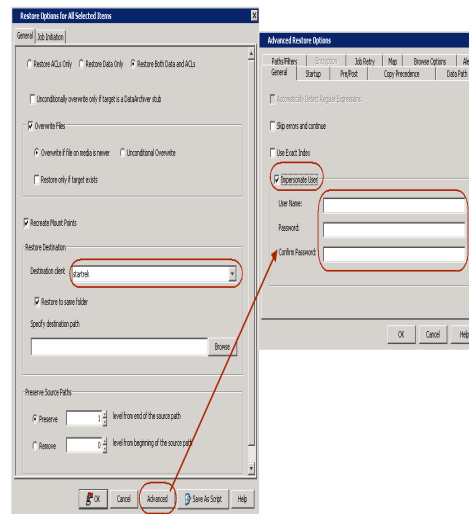
OVERWRITING DATA DURING RESTORES

Several options are available for overwriting data during data recovery operations. These options collectively provide greater control over what data should be overwritten during the data recovery operation, as well as the circumstances in which overwrites should occur.

By default, no overwrite options are selected for any data recovery operations. As such, data recovery operations behave as depicted in the following table:

If the data on the destination computer:	and the archived data:	then the archived data is:
has the same name as the archived data	is as old or older than the data on the destination computer	Not Restored
has the same name as the archived data	is newer than the data on the destination computer	Restored
has a different name than the archived data	has a different name than the data on the destination computer	Restored

By selecting any combination of overwrite options, the above behaviors will change in accordance with the particular overwrite options selected. Once the data recovery operation has completed, you can check the Restore Job History to view the data that was successfully restored.

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

2. Right-click the subclient in the right pane and then click **Browse**.

3. Click **OK**.

4. Select data that you want to restore and click **Recover All Selected**.

5. Ensure that the **Overwrite Files** check box is selected.

6. Click **Unconditional Overwrite**.

7. Click **OK**.
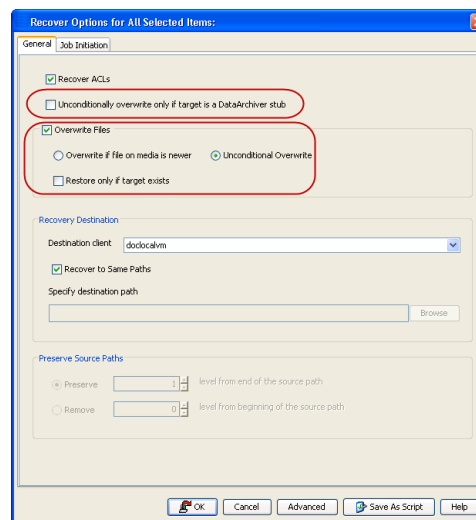
OVERWRITING DATA ONLY IF IT EXISTS ON THE DESTINATION

Follow the steps given below to restore the only data that already exists in the destination computer. This ensures any data removed from the destination computer is not reintroduced by the data recovery.

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

2. Right-click the subclient in the right pane and then click **Browse**.

3. Click **OK**.

4. Select data that you want to restore and click **Recover All Selected**.

5. Ensure that the **Overwrite Files** check box is selected.

6. Select the **Restore only if target exists** check box operation.

7. Click **OK**.
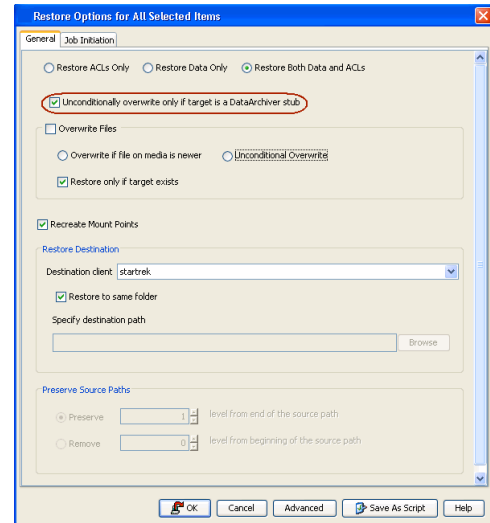
OVERWRITING DATA ONLY IF IT IS A STUB

Follow the steps given below to restore data and overwrite unconditionally if the data on the client computer is a stub. This ensures that only archived data is overwritten.

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

2. Right-click the subclient in the right pane and then click **Browse**.

3. Click **OK**.

4. Select data that you want to restore and click **Recover All Selected**.

5. Select the **Unconditionally overwrite only if the target is a DataArchiver stub** check box.

6. Click **OK**.
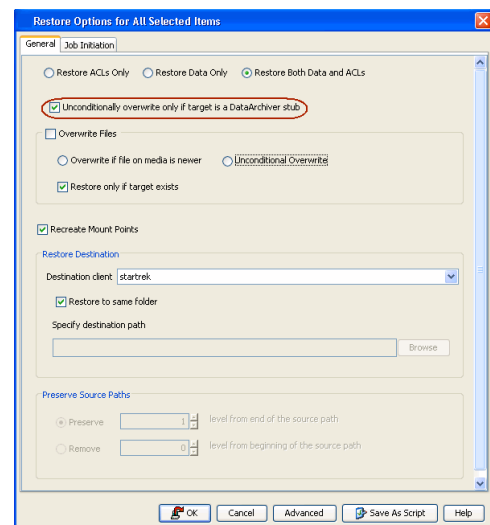
RESTORE BY JOBS

You can select a specific archive job for a restore. This method of restoring data is faster and useful in the following scenarios:

● To restore point-in-time data associated with a specific backup job

● To restore multiplexed data from the same client

RESTORING ALL THE DATA BACKED UP DURING A JOB

Following the steps to restore all the data archived during the selected job:

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

2. Right-click the **<Archive Set>** point to **All Tasks** and click **Restore by Jobs**.

3. Enter the **Start Time** and **End Time** and click **OK**. The list of backup jobs, completed in the specified time period is displayed.

4. Right click the job you wish to restore and click **Restore Selected Jobs.**

5. Click **OK**.
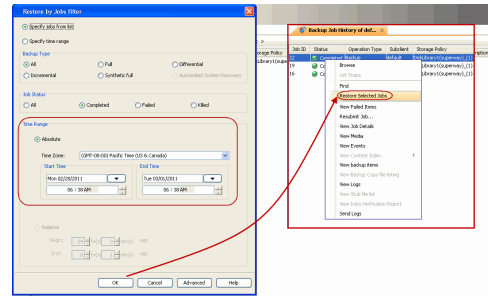
RESTORING SPECIFIC DATA BACKED UP DURING A JOB

You can restore specific files and folders from the data archived during the selected job. Follow the steps given below to restore specific files and folders from the selected archived job:

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

2. Right-click the **<Archive Set>** point to **All Tasks** and click **Restore by Jobs**.

3. Enter the **Start Time** and **End Time** and click **OK**. The list of backup jobs, completed in the specified time period is displayed.

4. Right click the job you wish to restore and select **Browse**.

5. Click **OK** in the **Browse Options** dialog box.

6. Select data that you want to restore and click **Recover All Selected**.

7. Click **OK** in the **Restore Options for All Selected Items** dialog box.
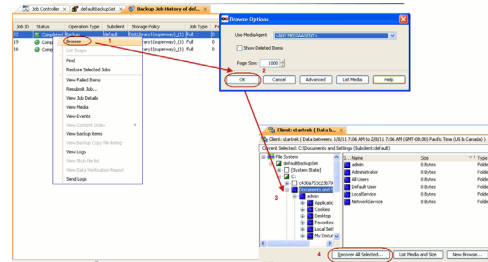
BROWSE AND RESTORE DATA

The option to browse the backup data provides the facility to view and selectively restore/recover the data that was backed up.

BROWSING THE LATEST DATA

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

2. Right-click the **Subclient** in the right-pane, point to **All Tasks** | **Browse**.

3. Click **OK**.

The browse option can also be invoked from the agent, archive set, or subclient level.
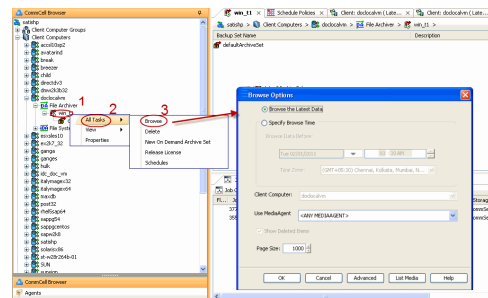
BROWSING DATA BEFORE A SPECIFIED TIME

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

2. Right-click the **Subclient** in the right-pane, point to **All Tasks** | **Browse**.

3. Select **Specify Browse Time** and the **Time Zone.**

4. Click **OK**.
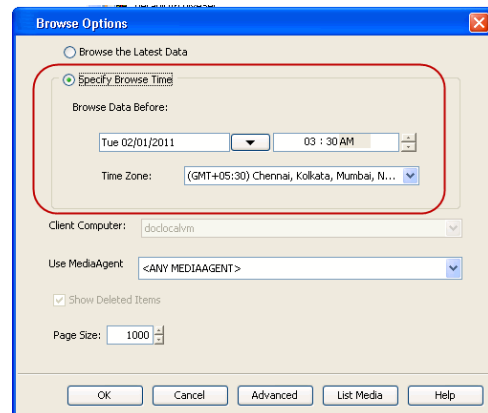
BROWSING DATA BETWEEN A SPECIFIED TIME

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

2. Right-click the **Subclient** in the right-pane, point to **All Tasks** | **Browse**.

3. Select **Specify Browse Time** and the **Time Zone.**

4. Click **Advanced.**

5. Select **Exclude Data Before,** select the date and time from which you wish to view the data in the browse window.

6. Click **OK**.
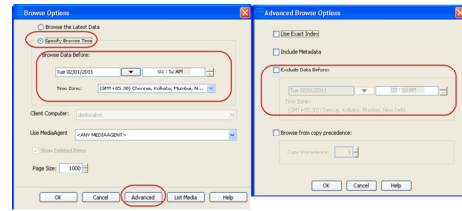
BROWSING MULTIPLE VERSIONS OF A FILE/OBJECT

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

2. Right-click the **Subclient** in the right-pane, point to **All Tasks** | **Browse**.

3. Click **OK**.

4. Expand the list of objects, right-click the file and click **View All Versions**.

5. From the list of date-stamped versions, select the version you want and click **Restore**.

6. In the next window, select recovery destinations and optionally, other recover options and click **OK**.

   - If all versions of a file are recovered, then the original file will remain a stub file and not be recovered.
   - Upon recovery, the system appends a unique number to the file name (file,1.txt; file,2.txt; where "1" is the most recent version, "2" is the next recent version, etc.) to ensure that different versions of a file residing in the same location have a unique name.
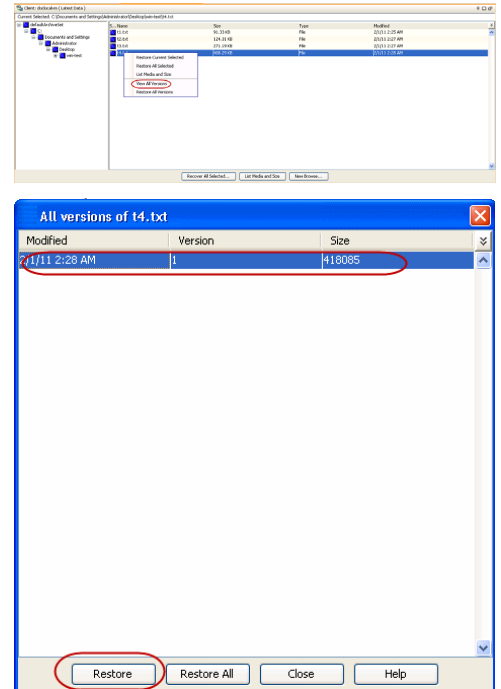
FINDING AND RESTORE

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**.
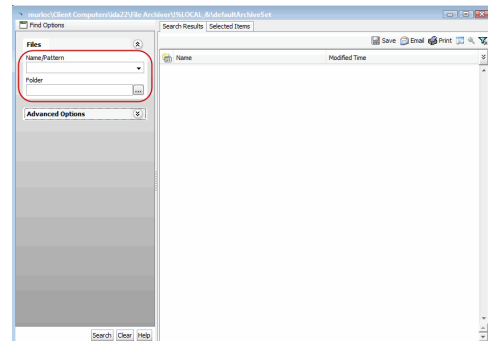
QUICK SEARCH USING SAMPLING

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**.
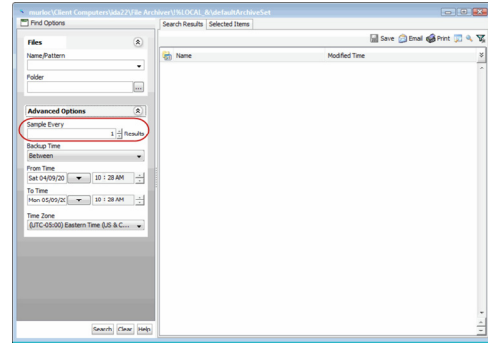
BY SPECIFIC TIME

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**.
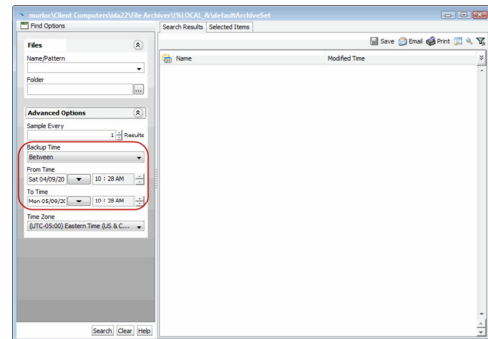
RESTORING ACLS

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

RESTORING ONLY THE ACLS

You can restore only the ACLs and apply it to an existing data in the destination. Follow the steps given below to restore only the ACLs and apply it to the existing files in the destination:

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 **Restore ACls Only**.

7. Click **Ok**.
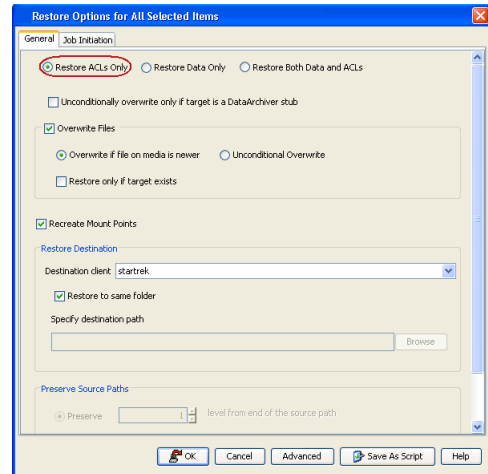
RESTORING ONLY DATA

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. Select **Restore Data Only**.

7. Click **Ok**.
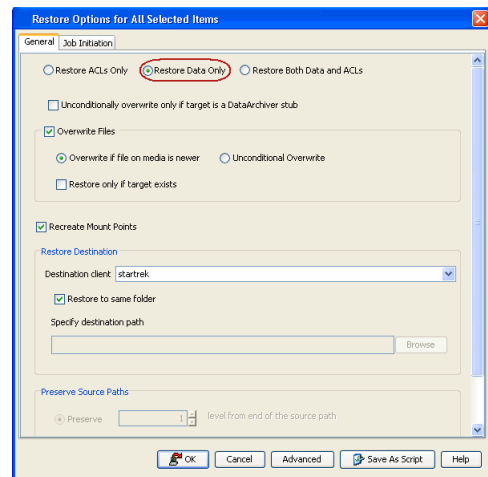
LISTING MEDIA

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 AN INSTANCE

1. From the CommCell Browser, right-click the instance for which you wish to list media, click **All Tasks** and then click **Browse**.

2. From the **Browse Options** dialog box, if required, select the following options:

   ○ Click **Browse the Latest Data** to list media associated with the most recent data protection cycle.

   ○ Click **Specify Browse Time** to list media associated with data protection operations up to the specified date and time range.

   Use the **Browse Data Before** box to specify the end date and time.

   ○ Click **Advanced** and then click **Exclude Data Before** and then select the date and time from which you wish to list media associated with data protection operations.

   Note that you can use the **Specify Browse Time** and **Exclude Data Before** options to list media between a specified date and time range.

3. Click **List Media**.

4. From the **List Media** dialog box, click **List Media for restore within specified time range** and click **OK**.

   The appropriate media is listed in the **Media** dialog box.

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.

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.

SCHEDULING A RECOVERY

1.
   - From the CommCell Console, navigate to **Client Computers | <Client> | File Archiver** .
   - Right-click an archive set point to **All Tasks** and click **Browse**.
   - Click **OK**.
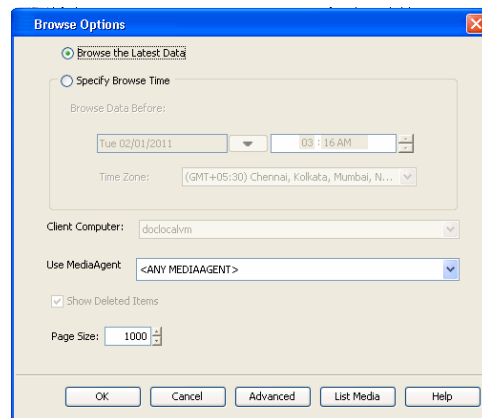
2.
   - Select data to restore.
   - Click **Recover All Selected**.
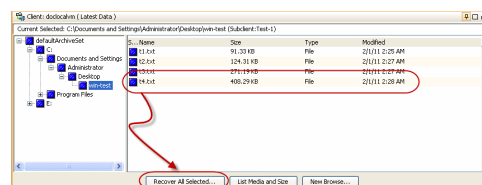
3.
   - Click **Job Initiation** tab and click **Schedule**.

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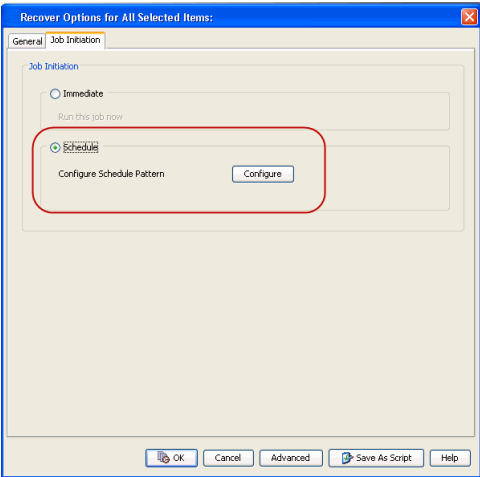
4. Select the appropriate scheduling options. For example:
   ● Click **Weekly**.
   ● Check the days you want the run the restore job.
   ● Change the Start Time to 9:00 PM
   ● Click **OK** to close the Schedule Details dialog
   ● Click **OK** to close the Restore Options dialog

   The restore job will execute as per the schedule.
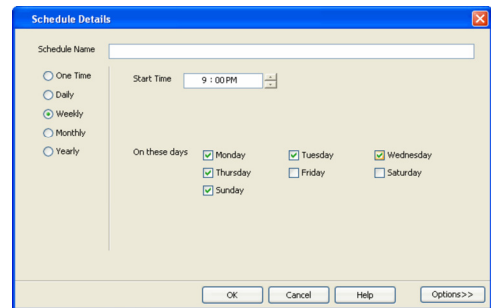
RESUBMITTING A RESTORE JOB

You can rerun a failed or completed restore job. This is useful when you want to use all the options and settings configured for the original job.

Follow the steps given below to rerun a restore job:

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

2. Right-click the **<Client>** and click **View | Job History**.

3. Select **Data Recovery**.

4. Select the **Restore** check box and clear all other check boxes.

5. Right-click the restore job that you want to resubmit from the **Data Recovery Job History** tab and click **Resubmit Job**.

6. Click **OK** in the **Restore Options for All Selected Items** dialog box.
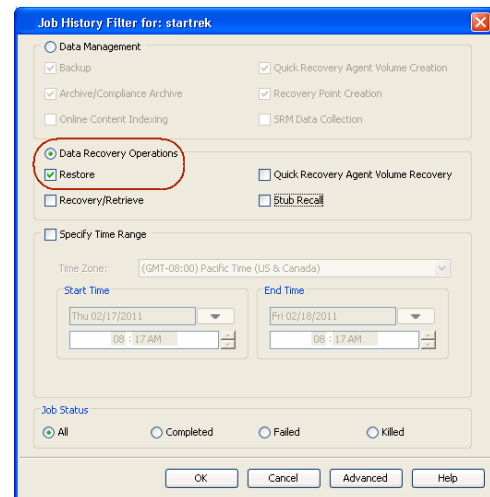
## MANAGE RECOVERY JOBS

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**.

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. Right-click the **Subclient** in the right-pane, point to **All Tasks | 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 the **Advanced** tab.

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

OPTION	DESCRIPTION	RELATED TOPIC
Skip Errors and Continue	This option allows a restore job to continue regardless of media errors and outputs a file that lists the full path names of the files that failed to get 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 Restore Options (General)** tab, select **Skip errors and continue** option. 7. Click **OK**.	
Use Exact index	This option allows the browse operation to use the index associated with the data protection operation performed at a specific time or the latest index. By default, the system uses the index associated with the most recent data protection operation. This option allows you to associate the media with the most recent index available in the CommCell. 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 Restore Options (General)** tab, select **Use Exact Index** option. 7. Click **OK**.	
Impersonate User	This information is needed only if you intend to restore data to a mapped network drive, shared network drive, or directory to which you do not have access privileges. You can impersonate a windows logon information with an account that has access rights to restore data. 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 Restore Options (General)** tab, select **Impersonate User** option.	
	7. In **User Name** and **Password** boxes, enter a user name and password which has access privileges. In **Confirm Password** box, type the password again.	
	8. Click **OK**.	
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.	Refer to Job Priority and Priority Precedence.
	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**.	
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.	Refer to Recovering Data From Copies.
	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**.	
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.	Refer to Change Data Path.
	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.	
	● 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**.
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.
Encryption	You can configure encryption for the specific subclient during the data recovery operation. You must configure encryption at the client level first and then at the subclient level to encrypt data during data recovery operations using the CommCell Console. Refer to Data Encryption.
	If you configure data encryption with a Pass-Phrase and do not elect to export the pass-phrase to destination clients, you will be required to enter the pass-phrase during immediate data recovery operations. Scheduled data recovery operations require you to export the pass-phrase.
	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 (Encryption)** tab, enter a pass-phrase in the **Pass Phrase** dialog box.
	7. Enter the pass-phrase again in the **Re-enter Pass Phrase** dialog box.
	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. Refer to Job Management.
	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**.
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.	Refer to Alert.
	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.**	
	10. Verify the **Summary**.	
	11. Click **Finish.**	
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 - NetApp File Archiver Agent

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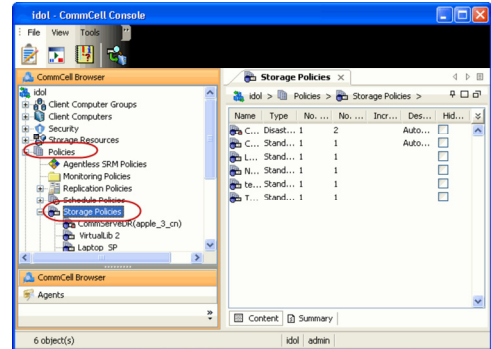
2. Highlight the **Storage Policy**.
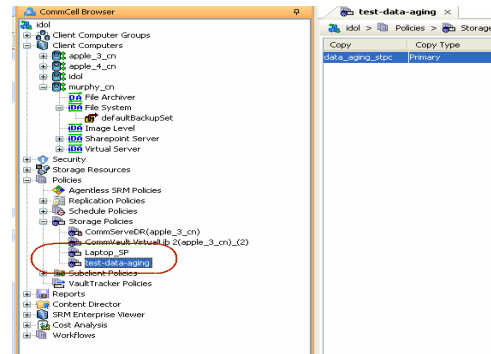
3. From the right pane, right-click the **Storage Policy Copy** and click the **Properties**.
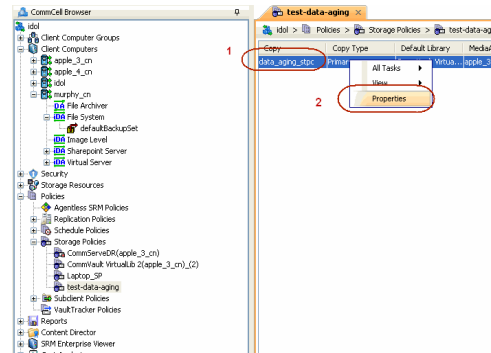
4.
- Click the **Retention** tab.
- Click the **Retain For** in the **Basic Retention Rules for All Backups** area.
- Enter number of days to retain the data.
- Enter number of cycles to retain the data.
- Click **OK**.
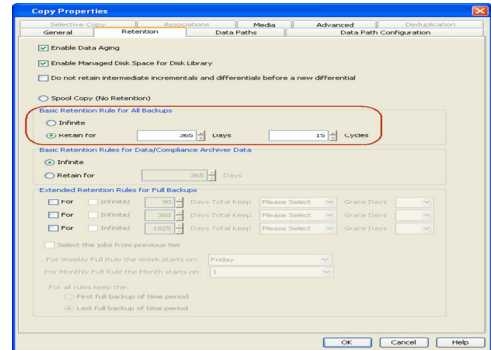
5. From the CommCell Browser, click the **Reports** icon.
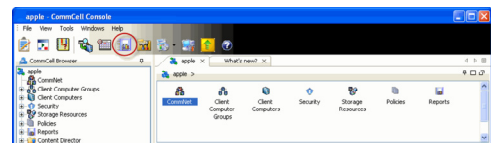
6. Expand Reports and select **Data Retention Forecast and Compliance.**
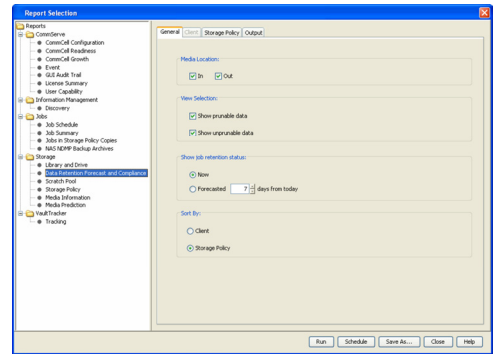
7. Click **Run**.
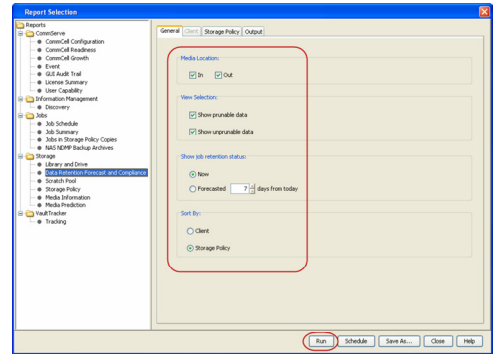
8. The report will display the data to be pruned when a data aging job is run.

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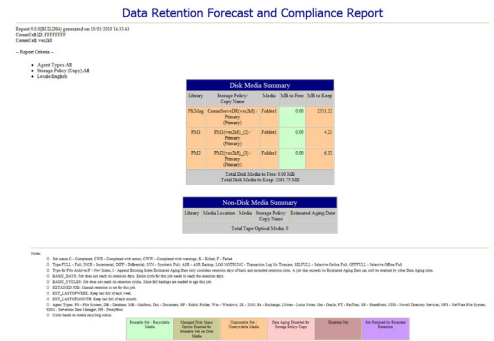
9. From the CommCell Console, right click the CommServe icon and click **All Tasks | Data Aging**.
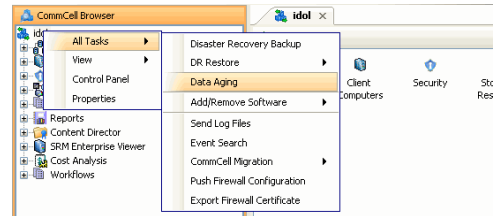
10. Select **Immediate** in the Job Initiation section and click **OK**.
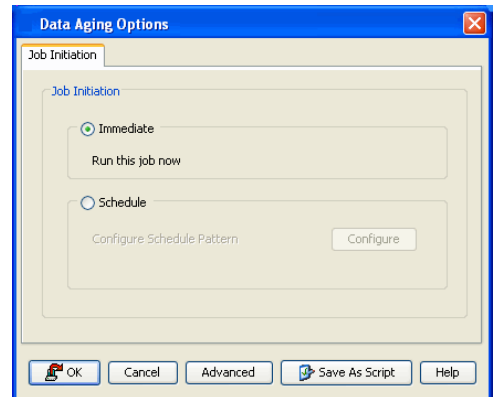
11. You can track the progress of the job from the **Job Controller** window. When the job has completed, the Job Controller displays **Completed**.
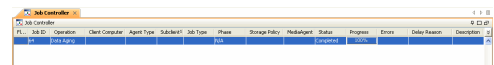
Make sure that the job completes successfully. If the job did not complete
successfully, re-run the job.

Additional Operations - NetApp File Archiver Agent

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

You can uninstall the components using one of the following method:

> Method 1: Uninstall Components Using the CommCell Console
>
> Method 2: Uninstall Components from Add or Remove Programs

METHOD 1: UNINSTALL COMPONENTS USING THE COMMCELL CONSOLE

1. From the CommCell Browser, right-click the desired Client Computer and click **All Tasks -> Add/Remove Programs** and click **Uninstall Software**.

2. **Uninstall Software Options** dialog will appear.

3. In the **Uninstall Software** tab, select **Uninstall All** to uninstall all the software packages.

4. In the **Job Initiation** tab, select **Immediate** to run the job immediately.

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

METHOD 2: UNINSTALL COMPONENTS FROM ADD OR REMOVE PROGRAMS

1. Click the **Start** button on the **Windows** task bar and then click **Control Panel**.

2. Double-click **Add/Remove Programs**.

   For Windows Vista/Windows 2008, click Uninstall a Program in the **Control Panel**.

3. Click **Remove** to uninstall the components in the following sequence:

   1. <Agent>

   2. File System *i*DataAgent

   3. Base Software

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

Back to Top

Archive Troubleshooting - NetApp File Archiver

| Archive | Recover |

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

STUB RECALLS FOR A RELOCATED MOUNT POINT DOES NOT WORK

PROBLEM CAUSE

If you archive data from a mount point, and if the mount point is subsequently relocated to some other path, stub recalls for this data will not work even the following operations are performed:

- If the services are restarted. Or,
- If a new mount point path is added in the registry and the services are restarted.

SOLUTION

Stub recalls from a relocated mount point will work only after the File Archiver for Windows client is rebooted. Therefore, be sure to reboot the client in this case.

UNABLE TO PRUNE 7.0 STUBS

PROBLEM CAUSE

After an upgrade from 7.0 to 8.0 or to 9.0, the data stubs that were created prior to the upgrade will not be pruned even after selecting the option to Prune Stubs After n Days.

SOLUTION

It is recommended to select the option to **Preserve stubs until the media has been pruned** to delete the 7.0 stubs post the media pruning operation.

RECENTLY MODIFIED FILES ARE NOT GETTING ARCHIVED

PROBLEM CAUSE

You may notice that the recently modified files are not getting archived during archiving phase because the time on the file server and that of the computer on which the file archiver agent is installed are not in sync.

SOLUTION

It is recommended to synchronize the file server time with the time of the computer on which File Archiver agent is installed.

ARCHIVE JOB MAY FREEZE

PROBLEM CAUSE

Archive job may freeze during the scan phase. For the frozen job to continue and complete successfully, restart GXHSMService.exe.

SOLUTION

If you are using Symantec Endpoint Protection 12, we recommend you to upgrade your version to 12.1.2 (RU2 MP1) (12.1.2100.2093) to resolve this issue.

RE-STUBBING OPERATION FAILS

If the proxy computer is running on Windows XP operating system, the re-stubbing operation might fail. This is because computers operating on Windows XP cannot automatically adjust the clock with the revised daylight savings time in November. When the file modification time is anywhere between November and March, re-stubbing may fail as there is a mismatch in the modification time of the files on the file server and the files residing in the stub cache folder in the proxy computer.

REGISTRY KEYS FOR MIGRATION ARCHIVING

Use the following registry keys to modify the default behavior of the Migration Archiver Agent:

TOPIC	REGISTRY KEY(S)	DESCRIPTION

Access and Modified Times	`GXHSMSERVICEKEEPTIMES`
	
	`GXHSMSTUBKEEPTIMES`
		Stub pruning looks at the archived time of the file to determine eligibility for pruning stubs. If you use the `GXHSMSERVICEKEEPTIMES` and `GXHSMSTUBKEEPTIMES` registry keys, the modified time will be preserved. This means that when you run a migration with these registry keys enabled, the preserved modified time will always be older than the time that the file was stubbed. The **Prune stub only after *n* days** is independent of the two registry keys.

	`GXHSM_PRESERVE_ACCESSTIME_ONMIGRTNS`
	
	`GXHSM_PRESERVE_ACCESSTIME_ONRECALLS`
		The access and modified times on files during migrations and recalls are preserved by default. You can stop preserving these times by using the `GXHSM_PRESERVE_ACCESSTIME_ONMIGRTNS` and `GXHSM_PRESERVE_ACCESSTIME_ONRECALLS` registry keys.

Access Control Lists (ACLs)	`GXHSMSERVICERESTOREACLS`	You can determine how to handle ACLs on a stub with regard to migration archiving. You can choose either to replace the original ACLs on the stub after migration archiving or to preserve the original ACLs on the stub. See `GXHSMSERVICERESTOREACLS` in Registry Keys for more information.
Log Files	`GXHSMSTUBLOGFAILFILESTRUNCATE`	You can determine whether the existing log file associated with your job should be truncated or appended to. See `GXHSMSTUBLOGFAILFILESTRUNCATE` in Registry Keys for more information.
Re-Stubbing	`GXHSMMAINTAINSTUBCACHE`	In order to speed up migration archiving operations, the software will or can attempt to re-stub files under the following conditions: ● The file must have been previously archived and then recalled by a non-browse recovery (i.e., stub recovery). ● The stub for this file must exist in the "stub cache directory". ● The Archive index must still exist in the system (i.e., was not removed by a data aging operation). ● The file must not have been modified after it had been recalled. In this case, during migration archiving, the system will simply swap the file for the stub in the stub cache, thereby speeding up the operation by not transferring or storing it again. This feature is enabled by default; however, it can be disabled by setting the `GXHSMMAINTAINSTUBCACHE` registry key value to `N`.
Stubs as Sparse Files	`GXHSMSTUBCREATESPARSE`	Stub files are created as sparse files by default so that the file system can utilize space more efficiently. However, if you would like to configure the system to create stub files that are not sparse files, then the value of the the `GXHSMSTUBCREATESPARSE` registry key must be set to `N`.
	`GXHSMIGNORESPARSE`	You can determine how to handle file migration archiving with regard to the sparse attribute. You can choose either to ignore the sparse attribute when archiving files or to archive only files without the sparse attribute set. See `GXHSMIGNORESPARSE` in Registry Keys for more information.
	However, if you have drives that are being monitored by VERITAS Storage Exec, ensure that `GXHSMIGNORESPARSE` is enabled to ensure that subsequent migration archiving jobs complete successfully and not just the initial migration archiving job.	

Stub Port Number	`EVMGRC_REMOTE_PORT_OVERRIDE`
	
	`EVMGRC_REMOTE_PORT`
		You can override the stub file port number by using the `EVMGRC_REMOTE_PORT_OVERRIDE` registry key. Use this key when the port number changes. Keep in mind that using this key defeats the benefit of being able to recall data using different port numbers for multiple Agents. When the key does not exist, the File Share Archiver client uses the stub content to determine port number. For 7.0 stubs, refer to the `EVMGRC_REMOTE_PORT` registry key.

Recover Troubleshooting - NetApp File Archiver

Archive | Recover

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

IMPROPER DATA DISPLAYED DURING RECOVERY OPERATIONS

PROBLEM CAUSE

The space quota for an object such as volume, directory or user is set lower than the amount already in use. Doing so may cause improper results for data protection or recovery operations.

SOLUTION

Do not set a quota for an object such as a volume, directory, or user that is lower than the amount that has already been used.

UNABLE TO RECALL FILES BY DOUBLE CLICKING THE STUBS

The presence of NetApp File Archiver on the same computer where the stubs exists may prevent from triggering a recall. It is recommended to recall FPolicy stubs through a mapped drive or UNC path.

UNABLE TO RESTORE FILES FROM A UNIX COMPUTER THAT WERE ARCHIVED FROM A WINDOWS COMPUTER

Ensure that both AD and NIS are configured on your NetApp file server. Also ensure that **usermap.cfg** file on the file server is set up so that the file server can map an AD user/group with NIS user/group.

Example

`"Bob Garg" == bobg` maps NT user Bob Garg to UNIX user bobg and vice versa

`mktg\Roy => nobody` allows mktg\Roy to login, but only with the privileges of UNIX user nobody

`engr\Tom => ""` disallows login by NT user engr\Tom

`uguest <= *` maps all other UNIX names to NT user request

`*\root => ""` disallows NT logins using the name root from all domains

PREVIEWING THE ARCHIVED FILES IS TRIGGERING A RECALL

In case the archived files are MAC files and their metadata has been archived then previewing them will cause the entire file and its metadata to be recalled.

RECALL FAILS WITH ACCESS DENIED ERROR

PROBLEM CAUSE

When you double click a stub to perform a recall, the recall operation fails with the message **Access Denied**. You will receive an error in the CommCell Console which says **Recall abort due to exported media. Afile-Data=[*number*].**

This happens because the Archiver Services perform a pre-check to see if the required media is available in the library.

SOLUTION

Import the required media into the library. We recommend you to have a latest backup cycle available always so that the stubs can be recalled from that cycle. Backup operations performed on disk libraries enable faster recalls as they are not bound by the read and seek rules binding to the tape drives.

BACKING UP STUBS LEADS TO A STUB RECALL

To protect FPolicy stubs it is recommended to use NAS NDMP *i*DataAgent.

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.

RECOVERING DATA ASSOCIATED WITH DELETED CLIENTS AND STORAGE POLICIES

The following procedure describes the steps involved in recovering data associated with the following entities:

- Deleted Storage Policy

- Deleted Client, Agent, Backup Set or Instance

BEFORE YOU BEGIN

This procedure can be performed when the following are available:

- You have a Disaster Recovery Backup which contains information on the entity that you are trying to restore. For example, if you wish to recover a storage policy (and the data associated with the storage policy) that was accidentally deleted, you must have a copy of the disaster recovery backup which was performed before deleting the storage policy.

- Media containing the data you wish to recover is available and not overwritten.

- If a CommCell Migration license was available in the CommServe when the disaster recovery backup was performed, no additional licenses are required. If not, obtain the following licenses:

    ○ IP Address Change license

    ○ CommCell Migration license

    See License Administration for more details.

- A standby computer, which will be used temporarily to build a CommServe.

RECOVERING DELETED DATA

1. Locate the latest Disaster Recovery Backup which contains the information on the entity (Storage Policy, Client, Agent, Backup Set or Instance) that you are trying to restore.

    ○ You can check the Phase 1 destination for the DR Set or use Restore by Jobs for CommServe DR Data to restore the data.

    ○ If the job was pruned and you know the media containing the Disaster Recovery Backup, you can move the media in the **Overwrite Protect Media** Pool. See Accessing Aged Data for more information. You can then restore the appropriate DR Set associated with the job as described in Restore by Jobs for CommServe DR Data.

    ○ If the job is pruned and you do not know the media containing the Disaster Recovery Backup, you can do one of the following:

    If you regularly run and have copies of the Data on Media and Aging Forecast report you can check them to see if the appropriate media is available.

2. On a standby computer, install the CommServe software. For more information on installing the CommServe, see CommServe Deployment.

3. Restore the CommServe database using the CommServe Disaster Recovery Tool from the Disaster Recovery Backup described in Step 1. (See Restore a Disaster Recovery Backup for step-by-step instructions.)

4. Verify and ensure that the **HDPS Client Event Manager HDPS Communications Service (EvMgrS)** is running.

5. If you did not have a CommCell Migration license available in the CommServe when the disaster recovery backup was performed, apply the IP Address Change license and the CommCell Migration license on the standby CommServe. See Activate Licenses for step-by-step instructions.

6. Export the data associated with the affected clients from the standby CommServe as described in Export Data from the Source CommCell.

    When you start the Command Line Interface to capture data, use the name of the standby CommServe in the –
    commcell argument.

7. Import the exported data to the main CommServe as described in Import Data on the Destination CommCell.

    This will bring back the entity in the CommServe database and the entity will now be visible in the CommCell Browser. (Press F5 to refresh the CommCell Browser if the entity is not displayed after a successful merge.)

8. If you have additional data that was backed up after the disaster recovery backup and before the deletion of the entity, use the procedure described in Import Metadata from a Tape or Optical Media to obtain the necessary information.

9. You can now browse and restore the data from the appropriate entity.

> As a precaution, mark media (tape and optical media) associated with the source CommCell as READ ONLY before performing a data recovery operation in the destination CommCell.

STUBS RECALLED AUTOMATICALLY

If you have PGP Disk Encryption tool used by SAP installed on your computer, you might find that the stubs (archived data) are recalled automatically without triggering a recall operation.

This is because certain permissions might be enabled in the **PGP Options** dialog box.

To resolve this issue, make sure that the **Overlay PGP icon on secured files and folders** and **Protect individual files** options are disabled in the **PGP Options** (**Netware** tab) dialog box.
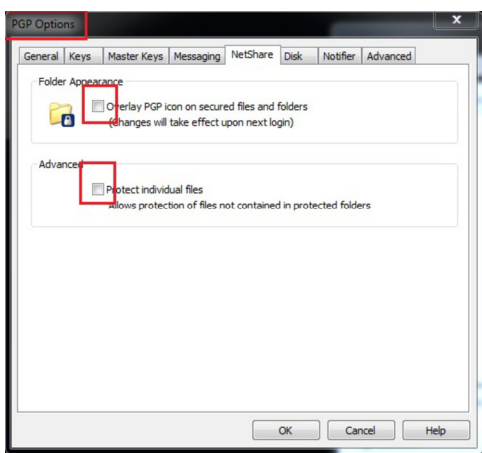
REGISTRY KEYS FOR RECOVERY OPERATIONS

Use the following registry keys to modify the default behavior of the Migration Archiver Agent:

TOPIC	REGISTRY KEY(S)	DESCRIPTION
Access and Modified Times	GXHSMSERVICEKEEPTIMES GXHSMSTUBKEEPTIMES	Migration archiving and stub recovery operations change the access and modified time on files. An enhancement that allows the recovery administrator to preserve the original file access time and modified time during migration archiving and stub recovery. See Registry Keys (GXHSMSERVICEKEEPTIMES and GXHSMSTUBKEEPTIMES) for more information on enabling this feature for all instance types except Celerra.
	GXHSMSERVICEKEEPTIMES GXHSMSTUBKEEPTIMES	Stub pruning looks at the modified time of the file to determine eligibility for pruning stubs. If you use the GXHSMSERVICEKEEPTIMES and GXHSMSTUBKEEPTIMES registry keys, the modified time will be preserved. This means that when you run a migration with these registry keys enabled, the preserved modified time will always be older than the time that the file was stubbed. As such, if you use the **Prune stub only after *n* days** option, you should ensure that the modified time is not being preserved. Therefore, be sure to disable the GXHSMSERVICEKEEPTIMES and GXHSMSTUBKEEPTIMES registry keys (which are enabled by default) when you use this option.
Stub Recalls	GXHSMSERVICEMINRECALLFREESPACE	If you would like to ensure that there is sufficient free space on a volume before initiating stub recalls, you can use the GXHSMSERVICEMINRECALLFREESPACE registry key to enable this feature.
	nRETRY_RECALL_TIMEOUT nRETRY_RECALL_DELAY	Two registry keys are available for administering the timing of recalls. 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. These keys work hand-in-hand with each other, and they are especially useful if the CommServe goes down.
	EVMGRC_REMOTE_PORT_OVERRIDE EVMGRC_REMOTE_PORT	For File Archiver for Windows, you can override the stub file port number by using the EVMGRC_REMOTE_PORT_OVERRIDE registry key. Use this key when the port number changes. Keep in mind that using this key defeats the benefit of being able to recall data using different port numbers for multiple Agents. When the key does not exist, the File Share Archiver client uses the stub content to determine port number. For 7.0 stubs, refer to the

		EVMGRC_REMOTE_PORT registry key.
	GXHSM_DISABLE_ARCHIVE_FILE_RECALL_AND_RESTORE	This registry key disables stub recalls at the driver level and allows service to send custom popup messages. This key should be used with a service level key GXHSM_DISABLE_ARCHIVE_FILE_RECALL_AND_RESTORE_MESSAGE. It is created in computers which has File Share Archiver Client installed.
	DMReadMaxMountRetryVal	By default no failure message is displayed when a recall job waits for the media to be imported. This key allows for setting a finite number of mount retries during restore.
Stub Recall History	nDMRSendFileStatus	The stub recall history is viewable at the client and agent levels in the Commcell Console and is associated with the first instance, which was created in the Migration Archiver agent. Stub recall history can be turned on by creating nDMRSendFileStatus key and setting the value to 1. You can use the nDMRSendFileStatus registry key to reduce the frequency at which the stub recovery job statistics are sent to Job Manager for updating the Recovery Job History views and reports. This is useful for increasing the efficiency of system resources in cases where there are frequent stub recalls and there is no need to update the Job History immediately after each stub recall.
	GXHSM_ENABLE_INPLACE_RESTORE	By default the recalls occur on a staged path, and then the recalled files are copied to the target path. This is a user defined key which allows the user to direct the recalls in place rather than the staging path.
	GXHSM_ALTERNATE_GXHSMCACHE_PATH	By default at the time of stub recall the stubs are stored in a stub cache path, which is generally in the root volume path. The Maximum supported path length for it is 1000. Any path longer than this specified length will get proportionately reduced if this key is specified. This user defined key allows the user to specify the path for all recalls.
Persistent Pipelines	nDMRSIDLETIMEOUT	To change the default value of how long the persistent pipeline of this Archiver Agent will stay open during idle periods of a recovery operation, you can use the nDMRSIDLETIMEOUT registry key to accomplish this task. The pipeline stays persistent for 24 hours by default. To ensure the registry key settings take effect, it is recommended that you restart the CommVault Client Event Manager Service (EvMgrc).
	nDMRMaxRestoreThreads	If you would like to spawn multiple persistent pipelines when stub recall requests are from different archive file IDs, the nDMRMaxRestoreThreads registry key can be used to accomplish this task.
Recall Messages and Pop-Ups	GXHSM_MAGNETIC_MSG_NAME	You can use the GXHSM_MAGNETIC_MSG_NAME key to replace the default "MAGNETIC" key word for a recall message with a message of your choice.
	GXHSMNOPOPUP	To enable the display of a pop-up message for stub recoveries indicating that the recovery operation has completed and showing the location of the file that was recovered, change the GXHSMNOPOPUP registry key value to N. To disable the pop-up, create the GXHSMNOPOPUP registry key and set the value to Y. It is recommended to use UNC based stub recalls on computers with Vista or Windows 2008. This is enabled by default on the local client for the File Archiver for Windows Agent when configured for NAS archiving. The GXHSMNOPOPUP registry key is not supported in Celerra proxy.
	GXHSM_DISABLE_ARCHIVE_FILE_RECALL_AND_RESTORE_MESSAGE	This is a service level key used in conjunction with the driver level key GXHSM_DISABLE_ARCHIVE_FILE_RECALL_AND_RESTORE on computers where File Share Archiver Cleint is installed. The key allows for customizing the popup message when GXHSM_DISABLE_ARCHIVE_FILE_RECALL_AND_RESTORE is used to disallow the recall. The key can be used with the following to get desirable popup messages: 1. "%s" can be used in the registry key value to represent the file name. 2. The popup message can be customized into top and bottom fields. Anything before <gxhd> would be message in the bottom field. Anything after <gxhd> will go in the top field. File %s is being recalled. <gxhd>Please wait....
	GXHSM_MAX_DISPLAY_TIME_FOR_DISABLERECALLRESTORE_MESSAGE	The key is used in conjunction with GXHSM_DISABLE_ARCHIVE_FILE_RECALL_AND_RESTORE_MESSAGE as it allows the user to set a desired popup message display time.
Log Files	GXHSMSTUBLOGFAILFILESTRUNCATE	For File Archiver for Windows, you can determine whether the existing log file associated with your job should be truncated or appended to. See GXHSMSTUBLOGFAILFILESTRUNCATE in Registry Keys for more information.

| Sparse Files | GXHSMSTUBCREATESPARSE | If you have enabled the archive option to create stub files that are not sparse files (using the GXHSMSTUBCREATESPARSE registry key), you must use WordPad — not Notepad — to open the resulting text files. |
| | GXHSM_NAS_REMOVESPARSE_ON_RECALL | In case of archiving FPolicy and Network File Share data, use GXHSM_NAS_REMOVESPARSE_ON_RECALL to remove the sparse attribute upon recall if the stub has been created as a sparse file. |

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.

Back to Top

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.

Back to Top

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.
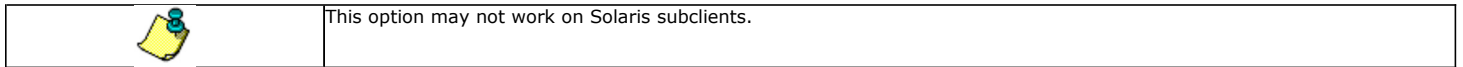
Expand symbolic links of subclient content

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.