Features - SharePoint Archiver Agent

TABLE OF CONTENTS

Overview - SharePoint Archiver Agent

Choose from the following topics:

- Introduction
- Supported Data Types
- Tree Levels in SharePoint Archiver
- License Requirement
- Configuration
- Archive and Recovery
- Disaster Recovery Considerations

INTRODUCTION

The SharePoint Archiver Agent is a software module responsible for periodically moving unused or infrequently used SharePoint documents on a host computer to secondary storage, thereby reducing the size of data on the primary storage. Archiver Agents reduce the duration of backup windows by reducing the amount of data to be backed up by an *i*DataAgent.

SUPPORTED DATA TYPES

SharePoint Archiver provides data protection support for documents from both versioned and non-versioned Document or Picture Libraries, except for those listed in the section below.

NOT SUPPORTED FOR ARCHIVING

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

- List items
- Other Library items (e.g., Form Library items)
- .ASPX files

TREE LEVELS IN SHAREPOINT ARCHIVER

When SharePoint Archiver is installed, the following levels are automatically created in the CommCell Browser.
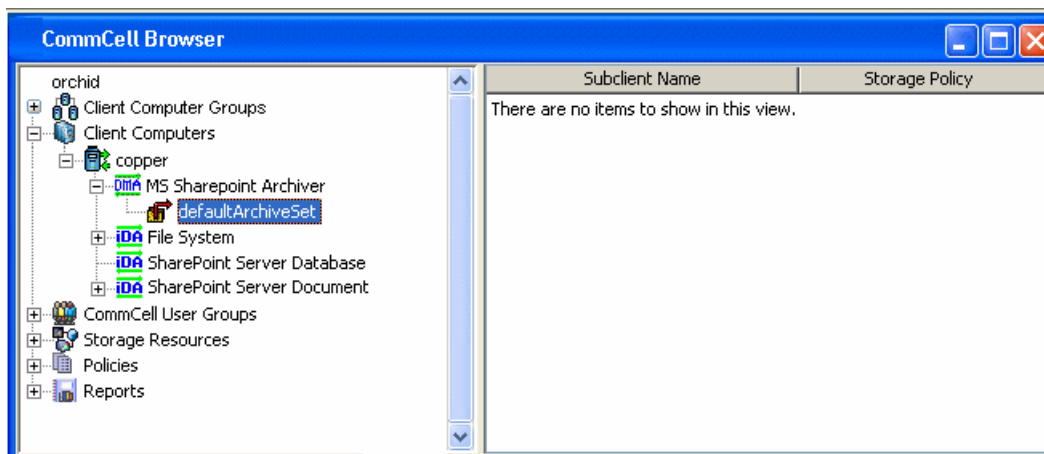
`copper:` Client

`MS SharePoint Archiver:` Agent

`defaultArchiveSet:` Archive Set

> Before performing a Migration Archiving Operation using a Archiver Agent, create a user-defined subclient. See Subclients - SharePoint Archiver for more information.

LICENSE REQUIREMENT

To perform a data protection operation using this Agent a specific Product License must be available in the CommServe® Server.

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

CONFIGURATION

ARCHIVING RULES

The configuration of the archiving rules is central to customizing migration archiving operations to meet the needs of your organization. The Archiving Rules are discussed in detail in Migration Archiving - SharePoint Archiver.

> Archiving Rules are initially disabled by default. After creating a subclient, you must clear the **Disable All Rules** option and configure archiving rules before Archive Operations are possible. Otherwise, the system will ignore all archiving rules (except for the Do Not Create Stub rule) for the subclient.

STORAGE POLICY

The retention criteria for preserving archived data through Storage Policies associated with Archiver Agents is based only on time, not cycles. For more information on Storage Policies, see Storage Policies.

ARCHIVE AND RECOVERY

MIGRATION ARCHIVING

After configuration is completed, migration archiving jobs can be scheduled. This is similar to scheduling backup jobs for *i*DataAgents. To ensure that only successfully archived files will be changed into stubs, the migration archiving operation is divided into two phases: archiving and stubbing. Stubs contain information about the archived data for recovery purposes. The stubbing phase starts after the archiving phase succeeds. However, stubs will only be created if the subclient properties were configured to create them during archiving.

> The database file that tracks the stubs is not backed up with the SharePoint Database *i*DataAgent. Therefore, you should back up this file with the Windows File System *i*DataAgent to ensure that stubs can be recovered. See Migration Archiving Considerations for details.

In the archiving phase, SharePoint Archiver will archive the files meeting the pre-set archiving criteria and, if applicable, put them into a list for the stubbing phase and prune expired stubs. Refer to Migration Archiving for more information on archiving.

RECALL OPERATIONS WITH MULTIPLE WEB FRONT END SERVERS AND DFS REPLICATION

When the SharePoint Archiver is installed on multiple Web Front End Servers, see Migration Archiving Considerations for configuration details and how to replicate SPDAStubDatabase.db across all Web Front End servers using Distributed File System (DFS) Replication.

RECOVERY

SharePoint Archiver provides two ways to recover an archived file: from the SharePoint Server User Interface or the CommCell Console (stand-alone application).

The first method of recovery is recovering archived file(s) from stub(s) in SharePoint Server. In the SharePoint Server User Interface, browse and select the item to restore, expand the **Edit** menu, and click **Recall Archived Data**.

> In the SharePoint Server User Interface, you can recover items only if **Yes** appears under the **Archive** column next to the item. If the **Archive** column is not visible after archiving, you may need to manually refresh the Browser.

The second method is from the CommCell Console. The browse of SharePoint Archiver data is forced to be a non-image browse to view all the archived files in this archive cycle (i.e., since last creation of new index). The administrator can browse and find the file to recover.

Refer to Recover Data - SharePoint Archiver - How To for more information on Recovery operations.

DISASTER RECOVERY CONSIDERATIONS

The SharePoint Archiver product does not provide the ability to restore the entire system in the event of a disaster. Systems using an Archiver Agent should also be protected using the corresponding backup and recovery agent. SharePoint Archiver relies upon the SharePoint Server database backup sets to perform

a full system restore of SharePoint data, and the Windows File System *i*DataAgent to restore the operating system. For more information, see Restore Data - SharePoint Server *i*DataAgents - Full System Restore.

If the stub database file (`SPDAStubDatabase.db`) is corrupted or if the `Job_Results` folder has moved to a new location, this database file should be restored with the Windows File System *i*DataAgent to the current `Job_Results` folder if it is not already present. If the database file is not corrupted but has moved location, you need to:

1. Copy the file to the new `Job_Results` folder location.

2. Modify the Distributed File System (DFS) Replication configuration to update the stub database file location when the SharePoint Archiver is installed on multiple Web Front End Servers.

Back to Top

System Requirements - SharePoint Archiver Agent

| System Requirements | Supported Features |

The following requirements are for the SharePoint Archiver Agent:

APPLICATION

Microsoft Office SharePoint Server 2007 up to the latest Service Pack
Microsoft SharePoint Server 2010
Microsoft SharePoint Foundation 2010
Microsoft SharePoint 2010 Standard and Enterprise
Microsoft Search Server 2010
Microsoft FAST Search Server 2010
Microsoft Search Server 2010 Express

OPERATING SYSTEM

WINDOWS SERVER 2008
Microsoft Windows Server 2008 32-bit and x64 Editions*

*Core Editions not supported

WINDOWS SERVER 2003
Microsoft Windows Server 2003 32-bit and x64 Editions* with a minimum of Service Pack 1

* Special configuration considerations apply. See Installing 32-bit Components on a Microsoft Windows x64 Platform for more information.

HARD DRIVE

103 MB minimum of hard disk space for software/ 148 MB recommended

50 MB of additional hard disk space for log file growth

717 MB of temp space required for install or upgrade (where the temp folder resides)

MEMORY

32 MB RAM minimum required beyond the requirements of the operating system and running applications

PROCESSOR

All Windows-compatible processors supported

PERIPHERALS

DVD-ROM drive

Network Interface Card

MISCELLANEOUS

NETWORK
TCP/IP Services configured on the computer.

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

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

DISCLAIMER

Minor revisions and/or service packs that are released by application and operating system vendors are supported by our software but may not be individually listed in our System Requirements. We will provide information on any known caveat for the revisions and/or service packs. In some cases, these revisions and/or service packs affect the working of our software.

Changes to the behavior of our software resulting from an application or operating system revision/service pack may be beyond our control. The older releases of our software may not support the platforms supported in the current release. However, we will make every effort to correct the behavior in the current or future releases when necessary. Please contact your Software Provider for any problem with a specific application or operating system.

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

Install - SharePoint Archiver Agent

TABLE OF CONTENTS

INSTALL REQUIREMENTS

The following procedure describes the steps involved in installing the SharePoint Archiver Agent. The SharePoint Archiver Agent should be installed on all Web Front End Servers of a Microsoft Office SharePoint Server or Windows SharePoint Services computer. The machine on which the SharePoint Archiver Agent is installed is referred to as the *Client* computer in this install procedure.

Verify that the computer in which you wish to install the software satisfies the minimum system requirements; refer to System Requirements - SharePoint Archiver Agent.

Review the following Install Requirements before installing the software:

GENERAL

- Review Install Considerations before installing the software.
- Agents should be installed only after the CommServe and at least one MediaAgent have been installed in the CommCell. Also, keep in mind that the CommServe® software and MediaAgent must be installed and running (but not necessarily on the same computer), before you can install the Agent.
- Close all applications and disable any programs that run automatically, including anti-virus, screen savers and operating system utilities. Some of the programs, including many anti-virus programs, may be running as a service. Stop and disable such services before you begin. You can re-enable them after the installation.
- Ensure there is an available license on the CommServe software for the Agent.
- Verify that you have the Software Installation Disc that is appropriate to the destination computer's operating system.
- If the SharePoint Server *i*DataAgent is installed on the same machine as the CommServe, Media Agent, or File Archiver for Windows, ensure that all services are running under the same SharePoint Administration Account that is specified below.

BEFORE YOU BEGIN

- Log on to the client as local Administrator or as a member of the Administrators group on that computer.

INSTALL PROCEDURE

GETTING STARTED

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

   After a few seconds, the installation program is launched.

   If the installation program does not launch automatically:

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

   NOTES

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

2. Choose the language you want to use during installation. Click the down arrow and select the desired language from the drop-down list, and click **Next** to continue.
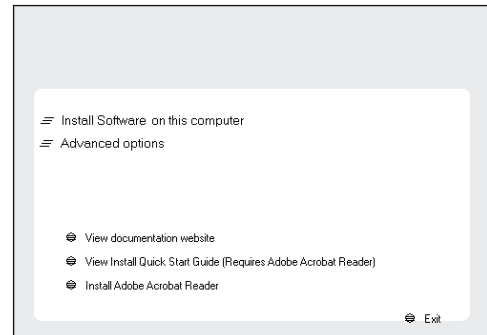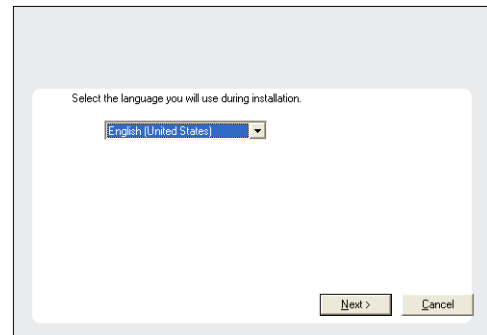
3. Select the option to install software on this computer.

    NOTES

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

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

    Click **Next** to continue.

SELECT COMPONENTS FOR INSTALLATION

5. Select the component(s) to install.

    NOTES

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

    Click **Next** to continue.

    To install the SharePoint Archiver agent expand the `Client Modules` folder, and the `Archive Management` folder, then select the following:

    ● `SharePoint Archiver Agent`
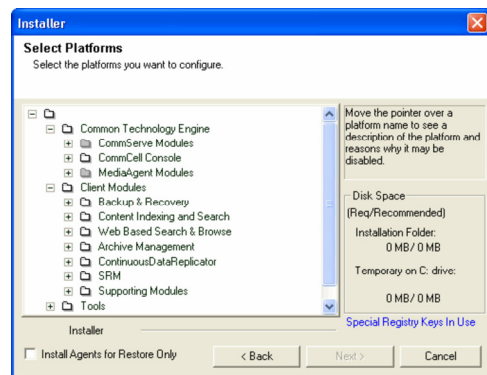
CONFIGURATION OF OTHER INSTALLATION OPTIONS

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

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

If firewall configuration is not required, click **Next** to continue.
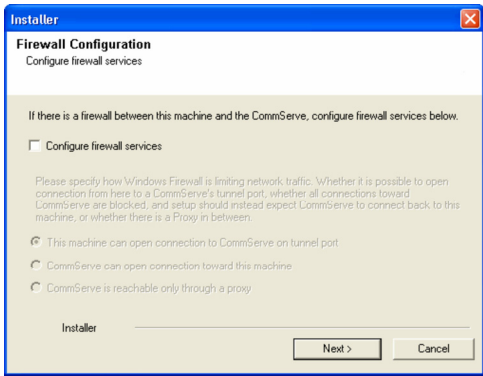
7. Enter the fully qualified domain name of the CommServe Host Name. This should be TCP/IP network name. e.g., computer.company.com.

NOTES

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

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

- If a computer has already been installed, this screen will not be displayed; instead the installer will use the same Server Name as previously specified.
- If you do not specify the CommServe Host Name, a window will be prompted to continue in decouple mode. Click **Yes** to continue to Decoupled Install. Click **No** to specify a CommServe Name and continue with the installation.

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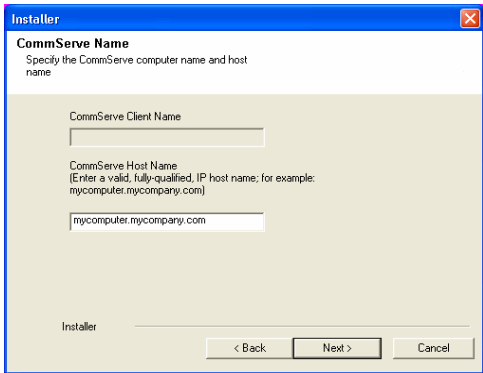
8. Enter the **username** and **password** associated with an external domain user account or a CommCell user account to authorize the installation of this agent.

NOTES

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

Click **Next** to continue.
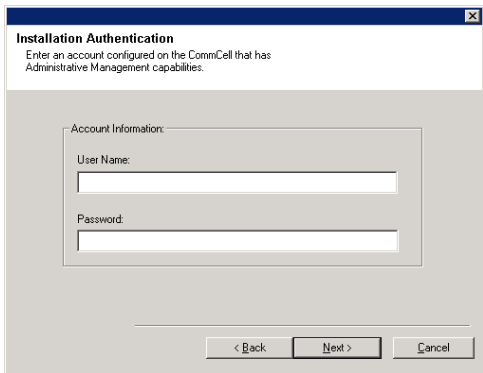
9. Enter the following:

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

NOTES

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

Click **Next** to continue.
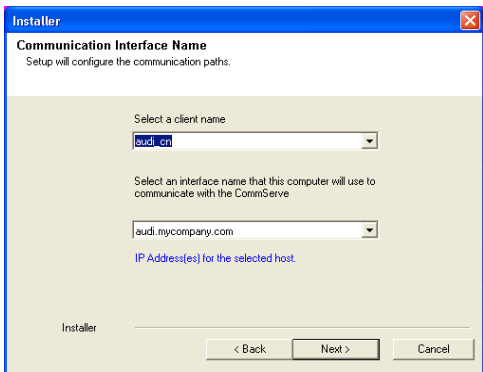
10. Select **Add programs to the Windows Firewall Exclusion List**, if you wish to add CommCell programs and services to the Windows Firewall Exclusion List.

NOTES:

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

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

Click **Next** to continue.
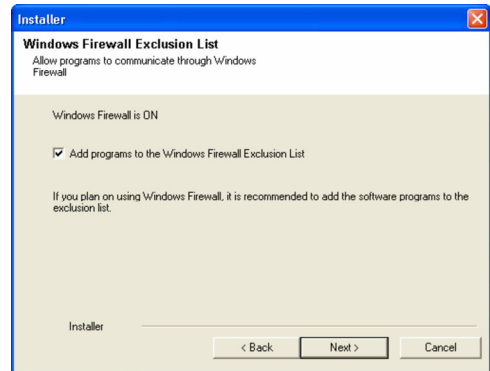
11. Specify the location where you want to install the software.

NOTES

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

Click **Browse** to change directories.

Click **Next** to continue.
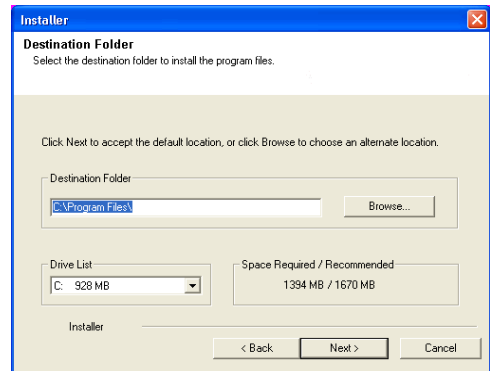
CLIENT GROUP SELECTION

12. Select a Client Group from the list.

Click **Next** to continue.

NOTES

- This screen will be displayed if Client Groups are configured in the CommCell Console. For more information, see Client Computer Groups.
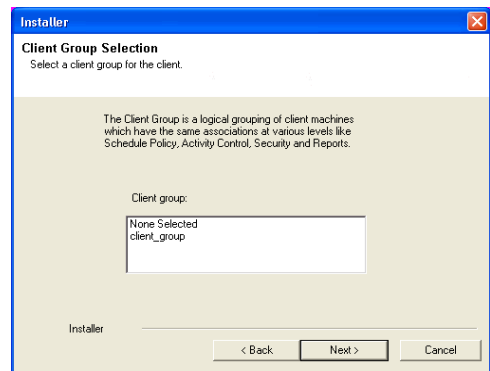
SCHEDULE AUTOMATIC UPDATE

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

NOTES

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

Click **Next** to continue.
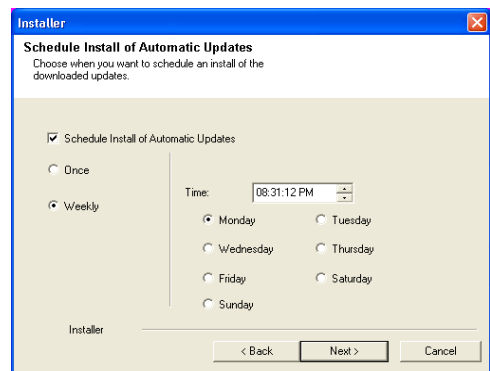
## STORAGE POLICY SELECTION

14. Select the storage policy through which you want to back up/archive the agent.

NOTES

- A storage policy directs backup data to a media library.
- If desired, you can change your storage policy selection at any time after you have installed the client software.
- This screen may appear more than once, if you have selected multiple agents for installation. You will be prompted to configure the storage policy association for each of the selected agents.

Click **Next** to continue.
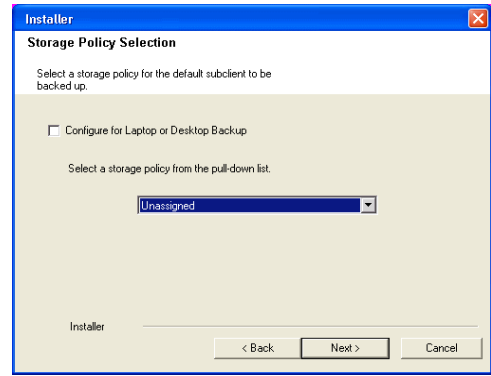
SHAREPOINT ADMINISTRATION ACCOUNT

15. Enter the User Name and Password for the SharePoint Administration Account.

Click **Next** to continue.

NOTES

The Base Services of the client will run under the user account that is specified. Use an account that meets this criteria:

- member of the local Administrator Group
- member of the SharePoint Administrator Group
- System Administrator role on the SQL Server Instance

In addition, this account must have "**Log on as Service**" permissions to ensure the Communication (CVD) Services will start. For more information on Base and Communication (CVD) Services, see Services.

Refer to the Knowledge Base article *Galaxy Service Account User Information for Windows 2003 and Window Server 2003 clients* available from the Maintenance Advantage web site.

See the SharePoint Agents section in **User Accounts and Passwords** for more information.

SHAREPOINT SERVER INFORMATION

16. You are prompted for the Microsoft SharePoint Server name. The computer name is displayed by default; if this is not correct, enter the correct name.

Click **Next** to continue.
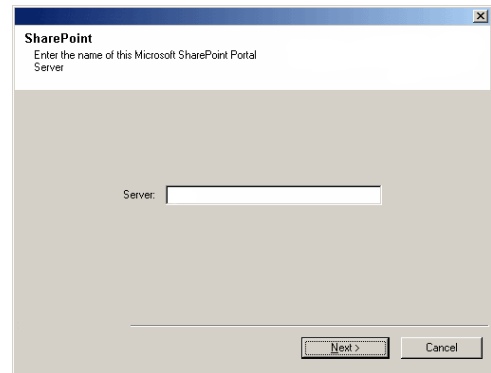
VERIFY SUMMARY OF INSTALL OPTIONS

17. Verify the summary of selected options.

NOTES

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

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

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

18.   Click **OK** to continue.
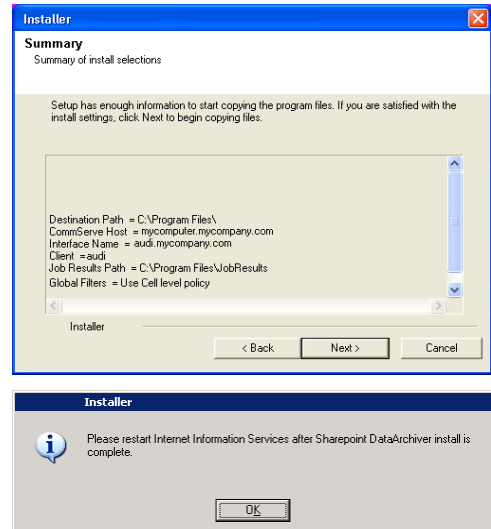
SETUP COMPLETE

19.   Click **Next** to continue.

NOTES

- Schedules help ensure that the data protection operations for the Agent are automatically performed on a regular basis without user intervention. For more information, see Scheduling.

20.   Setup displays the successfully installed components.

NOTES

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

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

The installation is now complete.
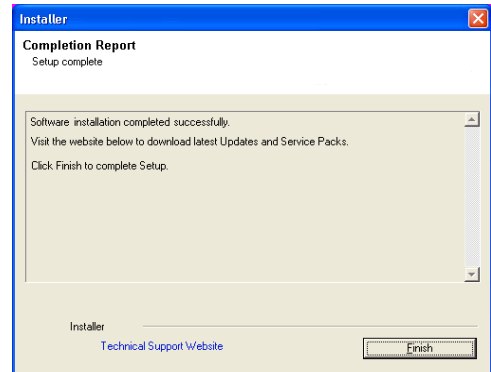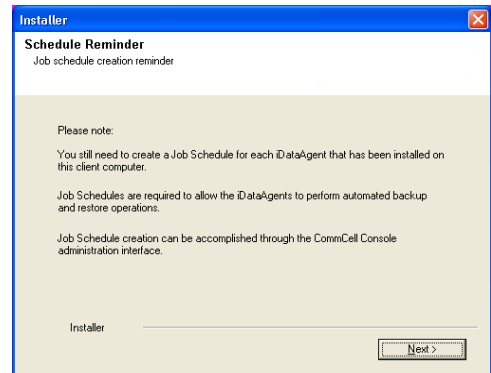
POST-INSTALL CONSIDERATIONS

GENERAL

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

Back to Top

Migration Archiving - SharePoint Archiver

Topics | How To | Related Topics

Overview

How to Set Up and Run a Migration Archive Operation

Migration Archiving Considerations

Advanced Archive Options

OVERVIEW

This section discusses archive information that is specific to the SharePoint Archiver Agent. See Migration Archiving for a general overview.

During archive operations, the SharePoint Archiver Agent will archive versioned and non-versioned documents that meet the preset criteria specified in the **Archiving Rules** tab of the **Subclient Properties** dialog box. Information about each archived object is placed into a stub (when enabled) that can then be used as a link to recover the data.

The configuration of the archiving rules is central to customizing archive operations to meet the needs of your organization. Continue on to the following section for an in-depth discussion of the archiving rules for these agents.

HOW TO SET UP AND RUN A MIGRATION ARCHIVE OPERATION

The following section provides the steps to set up and run a Migrate Archive Operation:

1. Enable the Archiving Rules for the subclient that contains the content you wish to archive. See Enable (Disable) Archiving Rules for step-by-step instructions.

    By default, this option is disabled. When selected, all archiving rules will be enabled except for Stub Rules.

2. Configure the Archiving Rules for the subclient. In particular, decide if you want to create stubs in your environment. Even if the Archiving Rules are disabled, the Stub Rules will apply. See Configure Archiving Rules - SharePoint Archiver Agent for step-by-step instructions.

3. Run an archive operation. See Start a Migration Archiving Operation for step-by-step instructions.
    ○ If stubs were created, end-users or applications can recover files with a non-browse recovery operation by simply opening the stub file, thereby causing it to be restored. (see Recover Data from SharePoint Server User Interface).
    ○ If stubs were not created, then you can perform a browse recovery with CommCell Console (see Recover Data from the CommCell Console.

MIGRATION ARCHIVING CONSIDERATIONS

Before performing any archive procedure, review the following information:

● When SharePoint Archiver archives data, it creates a database file to track the stubs that will appear in the SharePoint user interface. Stubs contain information about the archived data for recovery purposes. This file, `SPDAStubDatabase.db`, resides in the `Job_Results` folder and is not backed up with the SharePoint Database *i*DataAgent. Therefore, you should back up this file with the Windows File System *i*DataAgent to ensure that stubs can be recovered.

● For successful archiving and recovery, the user performing the operation must have write permissions to the `SPDAStubDatabase.db` file that resides in the `Job_Results` folder. Otherwise, you may receive the error `Failed to update database with new version number`.

● The SharePoint Archiver Agent should be installed on all Web Front End servers of a Microsoft Office SharePoint Server or Windows SharePoint Services computer in order to complete successful recalls. However, when SharePoint is configured with multiple Web Front End Servers, archive operations should be run from only one of the Web Front End servers. Therefore, the `SPDAStubDatabase.db` must be replicated across all Web Front End servers using Distributed File System (DFS) Replication. See Step-by-Step Guide for the Distributed File System Solution in Windows Server 2003 R2 for details. Skip the Deploying a Namespace section and follow the instructions in the Deploying DFS Replication section instead.

● Filters can be used in conjunction with the "Items That Failed" list on the data protection Job History Report to eliminate backup or archive failures by excluding items which consistently fail that are not integral to the operation of the system or applications. Some items fail because they are locked by the operating system or application and cannot be opened at the time of the data protection operation. This often occurs with certain system-related files and database application files.

● Set the dwDisableAutoDiscovery registry key to **1** if you want to disable auto-discovery of sites for user-created subclients.

● If all items in a Library with a Major and Minor Version setting are getting archived, the latest version will remain available and a stub will not be created.

- At the completion of an archive operation, the SharePoint Archiver checks for any new Cluster Servers. An alert can be configured to restart Internet Information Server (IIS) Services when new Cluster Servers are detected. See Alerts and Monitoring for more information.

- In a SharePoint environment with more than 500 site collections, it is recommended to increase the size and number of log files with the *<logfile>*_MaxLogFileSize and *<logfile>*_MaxLogFileBackups registry keys. Replace *<logfile>* with any desired name (e.g., SPDBBackup, SPDocBackup, SPDocArchive, etc.).

Back to Top

Migration Archiving - SharePoint Archiver Agent - How To

Topics | How To | Related Topics

Migration Archive Options

Enable(Disable) Archiving Rules

Configure Archiving Rules - SharePoint Archiver Agent

Schedule a Migration Archiving Operation

Start a Migration Archiving Operation

Advanced Migration Archive Options

Start a Migration Archiving Operation in the Suspended State

Start a Migration Archiving Operation on New Media

Start a Migration Archiving Operation that Creates a New Index

Start a Migration Archiving Operation that Marks the Media Full

Start a Migration Archiving Operation with a Set Job Priority

Start a Migration Archiving Operation with VaultTracking enabled

ENABLE (DISABLE) ARCHIVING RULES

Related Topics:

- See Overview for an introduction to the archiving rules and Migration Archiving Considerations for a list of considerations before you begin archiving with the SharePoint Archiver Agent.

- User Account and Password - SharePoint Agents

Before You Begin

- Do not change the archive rules of a subclient that is being archived.

Required Capability: Capabilities and Permitted Actions

▶ To enable the archiving rules of Archiver Agents:

1. From the CommCell Browser, right-click the subclient whose archiving rules you want to configure, then click **Properties** from the shortcut menu.

2. Click the Rules tab of the Subclient Properties.

3. Click the **Enable all rules** checkbox to enable rules-based migration archiving operations for this subclient. After enabling the rules, files will be archived based on the rules that are configured for the Agent.

4. Click **OK**.

CONFIGURE ARCHIVING RULES - SHAREPOINT ARCHIVER AGENT

Related Topics:

- Archiving Rules

Before You Begin

- Do not change the archiving rules of a subclient that is being archived.

Required Capability: Capabilities and Permitted Actions

▶ To configure archiving rules for the SharePoint Archiver Agent:

1. From the CommCell Browser, right-click the subclient whose archiving rules you want to configure, then click **Properties** from the shortcut menu.

2. Click the Archiving Rules tab of the Subclient Properties dialog box.

3. Clear the **Enable all rules** checkbox to disable rules-based migration archiving operations for this subclient. When this option is selected, all archiving rules will be ignored except for Stub Management rules. If you select this option, then go to Step 7, otherwise, for rules-based migration archiving operation, continue to the next step.

4. On the Document Rule tab:

   ○ In the **Archive documents whose Modified Time is older than the specified days** field, enter or select a value corresponding to the number of days elapsed since the last Modified Time of each document, in order for the document to be archived.

   ○ In the **Archive documents whose Size is greater than a specified threshold** field, enter or select a value corresponding to the size (in Kilobytes) a document must be in order for the document to be archived.

   ○ In the **Archive versions older than the last specified versions** field, enter or select a value corresponding to the number of versions that will be subtracted from the current version in order to archive the document.

   ○ You can optionally select the **Archive if: All of the above rules are satisfied** checkbox to archive a document if it satisfies ALL of the general criteria established above.

   ○ You can optionally select the **Archive if: Any of the above rules are satisfied** checkbox to archive a document if it satisfies one or more of the general criteria established above.

5. On the User tab:

   ○ You can **Add**, **Delete** or **Browse** SharePoint users for the **Archive documents whose owner is listed below** list to configure documents to be archived based on user ownership. This criteria is used in conjunction with the General and Type criteria to determine whether documents will be archived.

   ○ You can **Add**, **Delete** or **Browse** SharePoint site groups for the **Archive documents whose owner belongs to one of the site groups listed below** list to configure documents to be archived based on site group ownership. This criteria is used in conjunction with the General and Type criteria to determine whether documents will be archived.

6. On the Type tab, you can **Add** or **Delete** document types in the **Archive documents whose type is listed below** list to configure documents to be archived based on type. This criteria is used in conjunction with the General and Type criteria to determine whether documents will be archived. This criteria is used in conjunction with the General and Type criteria to determine whether documents will be archived.

7. On the Stub Rule tab, you can:

   ○ Optionally select the **Do not create stub** checkbox so that no stubs are created for archived documents.

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

SCHEDULE A MIGRATION ARCHIVING OPERATION

Required Capability: Capabilities and Permitted Actions

▶ To schedule a migration archiving operation of a selected subclient or archive set:

1. From the CommCell Browser, select one of the following:

   ○ To archive a subclient, right-click the subclient that you want to archive and click **Archive**.

   ○ To archive an archive set, right-click the archive set that you want to archive, click **All Tasks** and click **Archive All Subclients** or **Archive Default Archive Set**.

2. From the Archive Options dialog box, select when you want to run the job by clicking **Schedule**.

3. If you want to access the **Advanced Archive Options**, click the **Advanced** button.

4. After selecting when you want to run the job and any advanced options, click **OK**.

5. From the Schedule Details (Schedule Details) dialog box, create a schedule for this operation. See Create a Job Schedule for more information. Click **OK** to continue.

6. Your migration archiving operation will execute according to the specified schedule.

START A MIGRATION ARCHIVING OPERATION

The migration archiving process allows you to archive data immediately without having to wait for the scheduled archiving time.

Required Capability: Capabilities and Permitted Actions

▶ To start a migration archiving operation of a selected subclient or archive set:

1. From the CommCell Browser, select one of the following:

   ○ To archive a subclient, right-click the subclient that you want to archive and click **Archive**.

   ○ To archive an archive set, right-click the archive set that you want to archive, click **All Tasks** and click **Archive All Subclients** or **Archive Default Archive Set**.

2. From the Archive Options dialog box, select when you want to run the job by clicking **Run Immediately**.

3. If you want to access the **Advanced Archive Options**, click the **Advanced** button.

4. After selecting when you want to run the job and any advanced options, click **OK**. A migration archiving operation is started for selected subclient or archive set and indicates its status in the Job Controller window.

5. When the migration archiving operation has completed, a confirmation message will be displayed in the Job Controller window.

START A MIGRATION ARCHIVING OPERATION IN THE SUSPENDED STATE

Use the following procedure to start a migration archiving operation in the suspended state. For more information, see Start in Suspended State.

Required Capability: Capabilities and Permitted Actions

▶ To start a migration archiving operation of a selected subclient or archive set:

1. From the CommCell Browser, select one of the following:

   ○ To archive a subclient, right-click the subclient that you want to archive and click **Archive**.

   ○ To archive an archive set, right-click the archive set that you want to archive, click **All Tasks** and click **Archive All Subclients** or **Archive Default Archive Set**.

2. From the Archive Options dialog box, select when you want to run the job by clicking **Run Immediately**.

3. Click the **Advanced** button to access the **Advanced Archive Options**.

4. Click on the Advanced Archive Options (Startup) tab, and select **Startup in suspended state** and click **OK**.

5. After selecting when you want to run the job and any advanced options, click **OK**. A migration archiving operation is started for selected subclient or archive set and indicates its status in the Job Controller window.

6. When the migration archiving operation has completed, a confirmation message will be displayed in the Job Controller window.

START A MIGRATION ARCHIVING OPERATION ON NEW MEDIA

Before you Begin

● Use the following procedure to start a migration archiving operation on new media. For more information, see Start New Media.

● If you plan to archive SharePoint data with pass-phrase encryption, keep in mind that such data cannot be recovered from the SharePoint User Interface, but can only be recovered by performing a Browse and Recovery operation from the CommCell Console.

Required Capability: Capabilities and Permitted Actions

▶ To start a migration archiving operation of a selected subclient or archive set:

1. From the CommCell Browser, select one of the following:

   ○ To archive a subclient, right-click the subclient that you want to archive and click **Archive**.

   ○ To archive an archive set, right-click the archive set that you want to archive, click **All Tasks** and click **Archive All Subclients** or **Archive Default Archive Set**.

2. From the Archive Options dialog box, select when you want to run the job by clicking **Run Immediately**.

3. Click the **Advanced** button to access the **Advanced Archive Options**.

4. Click on the Advanced Archive Options (Media) tab, and select **Start new media** and click **OK**.
   If you would like jobs with other Job IDs to use this new media, also select the **Allow other schedule to use media set** option.

5. After selecting when you want to run the job and any advanced options, click **OK**. A migration archiving operation is started for the selected subclient or archive set and indicates its status in the Job Controller window.

6. When the migration archiving operation has completed, a confirmation message will be displayed in the Job Controller window.

START A MIGRATION ARCHIVING OPERATION THAT CREATES A NEW INDEX

Use the following procedure to start a migration archiving operation that creates a new Index. For more information, see Create New Index.

Required Capability: Capabilities and Permitted Actions

▶ To start an immediate migration archiving operation that will create a new index:

1. From the CommCell Browser, select one of the following:
   ○ To archive a subclient, right-click the subclient and click **Archive**.
   ○ To archive all subclients in an archive set, right-click the archive set, select **All Tasks** and click **Archive All Subclients** or **Archive Default Archive Set**. Click **Yes** to confirm.

2. From the Archive Options dialog box, select when you want to run the job by clicking **Run Immediately**.

3. Click the **Advanced** button to access the **Advanced Archive Options** dialog box.

4. Click on the Advanced Archive Options (Data) tab, click **Create new index** and click **OK**.

5. From the **Archive Options** dialog box, click **OK**. The migration archiving operation will begin and you can track the progress of the job in the Job Controller window.

6. When the migration archiving operation has completed, Job Controller displays Completed.

START A MIGRATION ARCHIVING OPERATION THAT MARKS THE MEDIA FULL

Use the following procedure to start a migration archiving operation that marks media full on completion. For more information, see Mark Media Full.

Required Capability: Capabilities and Permitted Actions

▶ To start a migration archiving operation of a selected subclient or archive set:

1. From the CommCell Browser, select one of the following:
   ○ To archive a subclient, right-click the subclient that you want to archive and click **Archive**.
   ○ To archive an archive set, right-click the archive set that you want to archive, click **All Tasks** and click **Archive All Subclients** or **Archive Default Archive Set**.

2. From the Archive Options dialog box, select when you want to run the job by clicking **Run Immediately**.

3. Click the **Advanced** button to access the **Advanced Archive Options**.

4. Click on the Advanced Archive Options (Media) tab, and select **Mark media full after successful operation** and click **OK**.

5. After selecting when you want to run the job and any advanced options, click **OK**. A migration archiving operation is started for selected subclient or archive set and indicates its status in the Job Controller window.

6. When the migration archiving operation has completed, a confirmation message will be displayed in the Job Controller window.

START A MIGRATION ARCHIVING OPERATION WITH A SET JOB PRIORITY

Use the following procedure to start a migration archiving operation with a set job priority. For more information, see Set a Job Priority.

Required Capability: Capabilities and Permitted Actions

▶ To start a migration archiving operation of a selected subclient or archive set:

1. From the CommCell Browser, select one of the following:
   ○ To archive a subclient, right-click the subclient that you want to archive and click **Archive**.
   ○ To archive an archive set, right-click the archive set that you want to archive, click **All Tasks** and click **Archive All Subclients** or **Archive Default Archive Set**.

2. From the Archive Options dialog box, select when you want to run the job by clicking **Run Immediately**.

3. Click the **Advanced** button to access the **Advanced Archive Options**.

4. Click on the Advanced Archive Options (Startup) tab, and select **Change Priority** and then enter a value. Click **OK** to continue.

5. After selecting when you want to run the job and any advanced options, click **OK**. A migration archiving operation is started for selected subclient or archive set and indicates its status in the Job Controller window.

6. When the migration archiving operation has completed, a confirmation message will be displayed in the Job Controller window.

START A MIGRATION ARCHIVING OPERATION WITH VAULTTRACKING ENABLED

Use the following procedure to start a migration archiving operation with VaultTracker enabled.

For additional information, see the following:

- VaultTracker
- VaultTracker Enterprise

Required Capability: Capabilities and Permitted Actions

To start a migration archive operation of a selected subclient or archive set:

1. From the CommCell Browser, select one of the following:
   - To archive a subclient, right-click the subclient that you want to archive and click **Archive**.
   - To archive an archive set, right-click the archive set that you want to archive, click **All Tasks** and click **Archive All Subclients** or **Archive Default Archive Set**.

2. From the Archive Options dialog box, select when you want to run the job by clicking **Run Immediately**.

3. Click the **Advanced** button to access the **Advanced Archive Options**.

4. Click on the **Vault Tracking** tab, and select the vault tracking options you want to use and click **OK**.

5. After selecting when you want to run the job and any advanced options, click **OK**. A migration archiving operation is started for selected subclient or archive set and indicates its status in the Job Controller window.

6. When the migration archiving operation has completed, a confirmation message will be displayed in the Job Controller window.

Back To Top

Recover Data - SharePoint Archiver Agent

Topics | How To | Troubleshoot | Related Topics

Overview

How to Setup and Run a Recovery Operation

Recover a File from SharePoint Server User Interface

Recovery Options

Job Restarts

Recovery Destinations

- In-Place Recovery
- Out-of-Place Recovery
- Cross-Application Recoveries

Recovery Considerations for this Agent

Support for SharePoint Server with 2003 & 2007 Sites

Related Reports

OVERVIEW

The SharePoint Archiver Agent supports the following types of recoveries:

- Non-Browse Recovery of archived documents from stubs accessible in the SharePoint User Interface.

> Note that stubs are not automatically refreshed in the SharePoint User Interface. A manual refresh is required to view stubs recovered to the Server if the **Archive** column is not visible.

> In the SharePoint User Interface, you can recover items only if **Yes** appears under the **Archive** column next to the item. If the **Archive** column is not visible after archiving, you may need to manually refresh the Browser, select View "All Documents" or "All Pictures".

> If the **Recall Archived Data** menu is not visible in the SharePoint User Interface, you may need to manually refresh the Browser or it may be because multiple versions of SharePoint Servers co-exist on the same client. See Support when SharePoint 2003 and 2007 Servers Co-exist for more information.

> Unless you have **Add/Update** permissions to the document, you will not be able to recall archived documents.

> Library columns **CommVault Stub** and **Archived** created by SharePoint Archiver should not be changed by the user.

- Browse and Recovery using the CommCell Console. Browse and recovery operations for SharePoint Archiver Agent can be performed from the client, agent, and backup set (i.e., archive set) levels in the CommCell Browser.

Recoveries can be performed in-place or out-of-place, and in certain scenarios cross-application and cross-platform recoveries are also supported. (See Recovery Destinations below for comprehensive information.)

When there is a problem with the SharePoint Server or the operating system of the client computer, full system restores may be required. The SharePoint Archiver Agent relies upon the corresponding SharePoint *i*DataAgent to perform a full system restore of SharePoint Server data. See Restore Data - SharePoint Server iDataAgents - Full System Restore for more information.

HOW TO SET UP AND RUN A RECOVERY OPERATION

The following section provides the steps to set up and run a Recovery Operation:

1. Enable the Archiving Rules for the subclient that contains the content you wish to archive. See Enable (Disable) Archiving Rules for step-by-step instructions and configure the Archiving Rules. In particular, decide if you want to create stubs in your environment. Even if the Archiving Rules are disabled, the Stub Rules will apply. See Configure Archiving Rules - SharePoint Archiver Agent for step-by-step instructions.

2. Run an archive operation. See Start a Migration Archiving Operation for step-by-step instructions.

3. Determine your Recovery Destinations.

4. Recover one or more files with a Browse and Recovery or non-Browse Recovery operation.

   o If stubs were created, end-users or applications can recover files with a non-browse recovery operation by simply opening the stub file, thereby causing

it to be restored. (see Recover Data from SharePoint Server User Interface).

○ If stubs were not created, then you can perform a browse recovery with CommCell Console (see Recover Data from the CommCell Console).

RECOVER A FILE FROM SHAREPOINT SERVER USER INTERFACE

There are several common methods for recovering an archived file. Users can provide a path to the archived files to be recovered from the CommCell Console, browse and recover archived files from the CommCell Console or, if the subclient is configured to create stubs, perform a non-browse recovery from the SharePoint Server User Interface. A non-browse recovery is any action that causes an open and read to be executed for the archived file, which automatically initiates a recovery operation. For example, you can select the **Recall Archived Data** menu and click on the data to view its contents.

> If a subclient is configured with the **Archive files only, do not create stub** archiving rule option enabled, the archived files will be removed from the computer and a stub recovery is not possible. To recover files that were archived using this option, perform the procedure to Recover Data from the CommCell Console.

For step-by-step instructions, see Recover Data from SharePoint Server User Interface.

Back to Top

RECOVERY OPTIONS

The SharePoint Archiver Agent offers a variety of options for recovering selected documents, which are available in the SharePoint Archiver Agent's **View All Versions** or **Recovery Options** dialog box in the CommCell Console. These options and their descriptions are as follows:

● **Restore** or **Restore All Versions**

The **Restore** option will recover the current version. The **Restore All Versions** option will recover all versions of a multi-versioned document to a Version Enabled Library.

ADVANCED RECOVERY OPTIONS

Advanced recovery options and their descriptions are as follows:

● **Skip Errors and Continue**

For index-based agents, this advanced recovery option enables a recovery job to continue despite media errors. This option also provides an output file that lists the full path names of the files that failed to recover.

● **Start Job in Suspended State**

Specifies that this job will start in the Job Controller in a suspended state and cannot run until the job is manually resumed using the **Resume** option. This option can be used to add a level of manual control when a job is started. For example, you could schedule jobs to start in the suspended state and then choose which scheduled jobs complete by resuming the operation started in the suspended state.

● **Change Priority**

This option allows you to manually set a job priority. This is useful if you have jobs that are very important and must complete, and/or jobs that can be moved to a lower priority. For more information, see Job Priorities and Priority Precedence.

● **Recover from copy precedence**

This option allows you to select the copy from which you wish to recover. For more information on Copy Precedence, see Recovering Your Data From Copies.

● **Use Library**

Specifies the name of the library that will be used to perform the restore operation. Use this option when you wish to restore using a specific library. For example, if you know that the media containing the data you wish to restore is available in a specific library.

● **Restore deleted items**

Specifies that the recovery operation will include data that was secured during all archive operations, including deleted items**.**

● **Specify Time Range**

Specifies to recover data within a specified time zone and time threshold.

● **Alert**

Allows you to configure an alert using the Alert Wizard for the recovery operation.

JOB RESTARTS

You can specify the maximum number of allowed restart attempts and the interval between restart attempts for all data retrieve jobs. For step-by-step

instructions, see Specify Job Restartability for the CommCell.

For more information on this subjects, see Restarting Jobs.

RECOVER A DOCUMENT FROM SHAREPOINT

In addition to browsing and recovering documents from the CommCell Console, the SharePoint Archiver Agents provide a method to allow end-users to selectively recover documents from SharePoint clients. If the subclient was configured to create stubs during migration archiving operations, users can initiate a recovery of a previously archived item. Refer to the online help for the steps involved in performing these type of recoveries.

> If a subclient is configured with the **Do not create stub** archiving rule option enabled, the archived items will be removed from the computer and a stub recovery is not possible. To recover items that were archived using this option, see the procedure to Recover a Document from the CommCell Console.

RECOVERY DESTINATIONS

By default, the SharePoint Archiver Agent recovers data to the client computer from which it originated; this is referred to as an in-place recovery. You can also recover the data to another Client computer in the CommCell. Keep in mind the following considerations when performing such recoveries:

- The destination client must reside in the same CommCell as the client whose data was archived.
- Note that when you perform recoveries other than in-place recoveries, the recovered data assumes the rights (i.e., permissions) of the parent directory.

The following section enumerates the types of recovery destinations that are supported by the SharePoint Archiver Agent. See Recover Options - Recover Destinations - Support for a list of Agents supporting each restore/recovery destination type.

IN-PLACE RECOVERY

- Same path/destination

When performing a non-browse recovery of archived data from a stub, keep in mind that the data can only be recovered in-place to the same path/destination on the same client from which the data was archived.

OUT-OF-PLACE RECOVERY

- Same path/destination

Keep in mind that out-of-place recoveries can only be accomplished via a Browse and Recovery operation from the CommCell Console.

CROSS-APPLICATION RECOVERIES

- Support for restoring/recovering/retrieving data from one application version to another generally follows the same compatibility support provided by the associated third-party application vendor, unless otherwise noted.
- Cross-application restores for library and list items to the same or higher SharePoint Server version are supported.

> For non-browse recovery of archived data from a stub on a lower to higher version of SharePoint Server, only out-of-place recoveries using the Same path/destination is supported.

RECOVERY CONSIDERATIONS FOR THIS AGENT

Before performing any recovery procedure for these agents, review the following information.

- If the item you want to recover was archived using the **Do not create stub** option or the stub was manually deleted after the archive, then use the procedure to Recover a Document from the CommCell Console to perform the recovery.
- The default timeout value for recalling data is five minutes. If a timeout error occurs, the timeout value can be increased by setting the registry key value nRecallTimeout.
- When SharePoint Archiver archives data, it creates a database file to track the stubs that will appear in the SharePoint user interface. Stubs contain information about the archived data for recovery purposes. This file, SPDAStubDatabase.db, resides in the Job_Results folder and is not backed up with the SharePoint Database *i*DataAgent. Therefore, you should back up this file with the Windows File System *i*DataAgent to ensure that stubs can be recovered.
- For successful archiving and recovery, the user performing the operation must have write permissions to the SPDAStubDatabase.db file that resides in the Job_Results folder. Otherwise, you may receive the error Failed to update database with new version number.
- If the stub database file (SPDAStubDatabase.db) is corrupted or if the Job_Results folder has moved to a new location, this database file should be restored with the Windows File System *i*DataAgent to the current Job_Results folder if it is not already present. If the database file is not corrupted but has moved location, you need to:

1. Copy the file to the new `Job_Results` folder location.

2. Modify the Distributed File System (DFS) Replication configuration to update the stub database file location when the SharePoint Archiver is installed on multiple Web Front End Servers.

- When both SharePoint 2003 and SharePoint 2007 servers co-exist on the same client with the SharePoint Agent, the subclient content needs to be properly configured.

  See Support when SharePoint 2003 and 2007 Servers Co-exist for more information.

- Items recovered from a version-enabled library are recovered to a *new* version.

- When restoring libraries with SharePoint Archiver, user-defined views are not restored. You should use SharePoint Document *i*DataAgent instead to restore views.

- Configuring version criteria in the Archiving Rules is not supported when recovering items from non version-enabled libraries. See Configure Archiving Rules - SharePoint Archiver Agent for more information.

- You will be unable to retrieve archive data if the software has been uninstalled or deconfigured.

SUPPORT WHEN SHAREPOINT 2003 AND 2007 SERVERS CO-EXIST

When both SharePoint 2003 and 2007 servers co-exist on the same client with the SharePoint Archiver Agent, the **Recall Archived Data** menu may not be visible in the SharePoint User Interface.

SHAREPOINT PORTAL 2003 SERVER DATA

If the **Recall Archived Data** menu is not visible for SharePoint Portal 2003 Server data:

1. Run the following command on the command line from the `<Software Installation Path>\Base` installation directory:

   CVAddSharePointMenu -c

2. Restart Internet Information Services (IIS).*

SHAREPOINT SERVER 2007 DATA

If the **Recall Archived Data** menu is not visible for SharePoint 2007 Server data after upgrading to SharePoint Server 2007:

1. From the CommCell Browser, browse any subclient content (Click **Browse** under the subclient **Content** tab.

2. A message "`SharePoint was upgraded from 2003 to 2007`" will be displayed.

3. Restart Internet Information Services (IIS).*

*Typically, the **iisreset** command is used to restart IIS.

RELATED REPORTS

RECOVERY/RETRIEVE JOB SUMMARY REPORT

The Recovery/Retrieve Job Summary Report provides a list of recovery or retrieve operations for a specified time period.

STUB RECALL JOB SUMMARY REPORT

The Stub Recall Job Summary Report provides a list of stub recall operations for a specified time period.

Back to Top

Recover Data - SharePoint Archiver - How To

Topics | How To | Troubleshoot | Related Topics

Recover Data from SharePoint Server User Interface

Recover Data from the CommCell Console

RECOVER DATA FROM SHAREPOINT SERVER USER INTERFACE

Before You Begin

- Review the general recovery requirements from What You Need to Know Before Performing a Recovery and any agent-specific recovery requirements from Recovery Considerations for This Agent prior to performing any recovery.

- This procedure can be used to recover only SharePoint data which have been configured to display stub icons.

- In the SharePoint User Interface, you can recover items only if **Yes** appears under the **Archive** column next to the item. If the **Archive** column is not visible after archiving, you may need to manually refresh the Browser, select View "All Documents" or "All Pictures".

- If the **Recall Archived Data** menu is not visible in the SharePoint User Interface, you may need to manually refresh the Browser or it may be because multiple versions of SharePoint Servers co-exist on the same client. See Support when SharePoint 2003 and 2007 Servers Co-exist for more information.

- Unless you have **Add/Update** permissions to the document, you will not be able to recall archived documents.

- Library columns **CommVault Stub** and **Archived** created by SharePoint Archiver should not be changed by the user.

- Items recovered from a version-enabled library are recovered to a *new* version.

Required Capability: None.

To recover data from the SharePoint Server User Interface:

1. Log in to your SharePoint site.

2. In the SharePoint Server User Interface, browse to the Library and select the archived SharePoint item which has **Yes** in the **Archive** column.

3. Expand the Item Edit menu and click **Recall Archived Data.**

4. The data that is available for recovery is displayed. Select one or more versions by selecting a checkbox in the **Recall** column and click **Recall Selected Versions** to continue.

    - If the document is from a version-enabled library, more than one version may be available for recovery.
      Otherwise, if the document is from a non version-enabled library, only one version will be available.
    - If an error occurs instead of viewing available versions, see Troubleshoot.

5. A Persistent Recovery job will be initiated on CommServe and a popup message "`[Filename] Recall completed successfully.OK`" is displayed when recovery has completed. Click **OK** to return to the **Document Library** page. To hide this dialog box, see Hide "Recall Completed Successfully" Dialog Box.

After the recovery has completed, you can click the data to view its contents.

    - For successful archiving and recovery, the user performing the operation must have write permissions to the `SPDAStubDatabase.db` file that resides in the `Job_Results` folder. Otherwise, you may receive the error `Failed to update database with new version number.`
    - The default timeout value for recalling data is five minutes. If a timeout error occurs, the timeout value can be increased by setting the registry key value nRecallTimeout.

RECOVER DATA FROM THE COMMCELL CONSOLE

Before You Begin

- Review the general recovery requirements from What You Need to Know Before Performing a Recovery and any agent-specific recovery requirements from Recovery Considerations for these Agents prior to performing any recovery.

Required Capability: See Capabilities and Permitted Actions

To Recover data from the CommCell Console:

1. From the CommCell Browser, right-click the archive set that contains the data that you want to recover, click **All Tasks** and then click the available **Browse** command (command names vary by agent).

2. Run a browse operation. See Browsing Data - Migration Archiver Agents - How To for a list of customized browse operations and their step-by-step instructions. If you accept all defaults, you will be browsing the latest migration archiving operations for the selected data.

3. From the Browse window, select the data that you want to recover, then click **Recover All Selected**. See Select Objects From the Browse Window for Recovery for more information.

4. From the Recover Options for All Selected Items (General) dialog box, select **Restore All Versions** to recover the SharePoint items.

5. From the Advanced Recovery Options dialog boxes, select the recovery options that you want to use. For agents with multiple tabs, do not click **OK** until you have used all of the desired tabs. When you accept all the default settings, you will be recovering the selected data to its original location.

6. When recovering encrypted data, refer to Data Encryption for comprehensive feature information and procedures for using the Encryption tab of the Advanced Recovery Options dialog box.

7. After completing your selections, you can either start an immediate recovery or schedule the recovery.

   ○ If you want to schedule the job, click the Job Initiation tab from the Recovery Options dialog box, click **Schedule**, schedule the job, and then click **OK**.

   ○ If you want to run the job now, accept or click **Run Immediately** in the same tab and then click **OK**.

   While the job is running, you can right-click the job in the Job Controller and select **Detail** to view information on the job. After the data has been recovered, you will see a job completion message in the Job Controller and Event Viewer.

Back To Top

Agents - SharePoint Archiver

Topics | How To | Related Topics

Configurable Properties

- Activity Control
- Assigning a Filter Storage Policy for Erase Data by Browsing
- User Accounts
- User Security
- Version
- Stub Rule

CONFIGURABLE PROPERTIES

Once installed, the agent is configured and is therefore able to manage the data on the client computer. However, you can change certain aspects of the configuration (e.g., client computer, backup sets, etc.) to manage the data in the manner that best suits your needs. Depending on the agent, you can view or change the agent configuration from the available tabs of the agent Properties dialog box.

ACTIVITY CONTROL

You can enable or disable all operations for this CommCell object and all objects below it. For more information, see Activity Control.

ASSIGNING A FILTER STORAGE POLICY FOR ERASE DATA BY BROWSING

A filter storage policy must be assigned to the agent in order to conduct Erase Data by Browsing operations. The purpose of the filter storage policy is to tell the system which media will be used to store the index filter information and how long to retain it. If one is not assigned at the time an Erase Data by Browsing job is run, the system will display a message reminding you that no filter storage policy has been defined. For step-by-step instructions, see Assign a Filter Storage Policy for Erase Data by Browsing.

USER ACCOUNTS

The **General** tab allows you to change the SharePoint account that is associated with SharePoint Archiver. This account was entered during installation of this Agent.

The Base Services of the client will run under the user account that is specified. Use an account that meets this criteria:

- member of the local Administrator Group
- member of the SharePoint Administrator Group
- System Administrator role on the SQL Server Instance

In addition, this account must have "**Log on as Service**" permissions to ensure the Communication (CVD) Services will start. For more information on Base and Communication (CVD) Services, see Services.

Refer to the Knowledge Base article *Galaxy Service Account User Information for Windows 2003 and Window Server 2003 clients* available from the Maintenance Advantage web site.

See the SharePoint Agents section in **User Accounts and Passwords** for more information.

USER SECURITY

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.

For more information, see User Administration and Security.

VERSION

The **Version** tab displays the software version and post-release service packs and updates installed for the component. See Version for an overview.

STUB RULE

Optionally, configure stub rules to manage the pruning of stubs. Stub creation rules are supported by all Migration Archiver Agents. If stub rules are not enabled, performing a stub recovery will not be possible.

These rules determine how long the stubs are retained and they assume that placeholder stubs are created when documents are archived. They apply to all subclients configured for this Agent.

- **Preserve stubs until the media has been pruned**

  When this rule is enabled, stubs will not be pruned until the media is aged during a data aging operation. Recovery of data is not possible when this rule is enabled.

- **Prune stub only after *n* days**

  When this rule is enabled, stubs will be retained for the specified number of days before it is pruned. This rule can be specified with different values for each subclient, but the rule for the subclient that has the lowest value will be the rule that is followed by all subclients.

Agents - SharePoint Archiver - How To

Topics | How To | Related Topics

Assign a Filter Storage Policy for Erase Data by Browsing

Browse the Latest Data

Change the SharePoint Administrator Account

Change Account for Executing Pre/Post Commands (Data Protection)

Run Erase Data by Browsing Job

Release License for Client, MediaAgent, Agent, or Enabler

Delete the Agent

View the Software Version

Configure Stub Rule

ASSIGN A FILTER STORAGE POLICY FOR ERASE DATA BY BROWSING

Before You Begin

- Acquire an Erase Data license.
- For an overview of all steps, see Erase Data by Browsing.
- Ensure that the filter storage policy that you associate with the agent for the Erase Data by Browsing feature has retention criteria that is greater than or equal to the retention criteria of the storage policy for the data to be erased.

Required Capability: See Capabilities and Permitted Actions

To assign a filter storage policy for Erase Data by Browsing:

1. From the CommCell Browser, right-click the appropriate agent icon and then click **Properties**.

2. From the Storage Device tab of the agent Properties dialog box, select a filter storage policy from the **Filter Storage Policy** list.

3. Click **OK**.

BROWSE THE LATEST DATA

The following procedure can be used to browse data from the client, agent, instance, backup set, replication set, or subclient level, depending on the functionality of a given agent.

Required Capability: See Capabilities and Permitted Actions

To browse the latest data:

1. From the CommCell Browser, right-click the level whose data you want to browse, click **All Tasks**, and then click the **Browse/Browse Backup Data** option from that level.

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

CHANGE THE SHAREPOINT ADMINISTRATOR ACCOUNT

Required Capability: See Capabilities and Permitted Actions

► To change the SharePoint Administrator Account:

1. From the CommCell Browser, right-click the agent icon of the client computer whose agent configuration you want to change, and then click **Properties**.

2. From the General tab of the agent **Properties** dialog box, click **Change Account**. In the Change Administrator Account dialog box, enter the new SharePoint Administrator Account and account password.

CHANGE ACCOUNT FOR EXECUTING PRE/POST COMMANDS (DATA PROTECTION)

Required Capability: See Capabilities and Permitted Actions

► To change a user account for executing pre/post commands for Data Protection jobs:

1. From the CommCell Browser, expand the tree to view the appropriate level icon for the affected agent.
   ○ From the agent, instance/partition, or backup set/archive set level, right-click the appropriate icon, click **All Tasks**, and click **New Subclient** from the short-cut menu.
   ○ From the subclient level, right-click the subclient icon and click **Properties** from the short-cut menu.

2. From the Subclient Properties dialog box, create and/or configure the subclient as appropriate. Then click the **Pre/Post Process** tab.

3. From the **Pre/Post Process** tab, click **Change**.

4. From the User Account dialog box, select one of the account options. If you select **Impersonate User**, type the appropriate user name and password.

5. Click **OK** to save the settings.

RUN ERASE DATA BY BROWSING JOB

Before You Begin

● Ensure there is a Filter Storage Policy configured for the agent in the Agent Properties (Storage Device) tab.

● An Erase Data license must exist.

Required Capability: Capabilities and Permitted Actions

► To erase data by browsing:

1. From the CommCell Browser, right-click the agent that contains the data which you want to erase, select **All Tasks** and then click **Erase Data By Browsing**.

2. You are warned that the data will be permanently removed. Click **Yes** to continue.

3. From the Erase Backup/Archived Data dialog box, perform one of the following tasks as appropriate for your agent:
   ○ Click **Add**, then specify the path of a data object that you want to erase, and click **OK**.
   ○ Click **Browse**, then select a browse time range and any advanced browse options, and click **OK**. From the browse selection window, select the data objects that you want to erase, and click **OK**.

4. Optionally, you can click **Add Alert** to configure an alert for this job.

5. Click **Schedule** if you would like to schedule this job, otherwise it will run immediately by default.

6. If you want to run the job immediately, click **OK** and the Erase Data by Browsing job will begin. When the job is done, Job Controller displays Completed.

7. If you selected Schedule, from the Schedule Details (Schedule Details) dialog box, create a schedule for this operation. Click **OK** to continue. Your Erase Data by Browsing operation will execute according to the specified schedule. See Create a Job Schedule for more information.

RELEASE LICENSE FOR CLIENT, MEDIAAGENT, AGENT, OR ENABLER

Required Capabilities: Capabilities and Permitted Actions

Administrative Management capability cannot be used to release the license from the MediaAgent level.

Before you Begin:

- To release license for MediaAgent, ensure that all the storage policies or copies associated with the configured libraries (or drive pools) in the MediaAgent are deleted or re-associated to another MediaAgent.

To release license for client, MediaAgent, agent, or enabler:

1. In the CommCell Browser, right-click the name of the client, MediaAgent, agent, or enabler you want to release license, click **All Tasks** (if displayed), and select **Release License**.

2. A popup warning message appears.

   Click **OK** to continue.

3. Another popup message then appears.

   Click **Yes** to continue with the deconfiguration or **No** to abort.

4. If releasing a license is unsuccessful, a number of popup messages appears. In some cases, the message requests that you take some corrective action. For example, the message might advise you to ensure that there are no jobs running on the agent. In such a case, click **OK** and take the appropriate action. Then repeat the process.

If releasing a license is successful, the tree element is dimmed and available for deletion.

DELETE THE AGENT

BEFORE YOU BEGIN

You can perform agent operations as long as the agent is installed and appears enabled in the CommCell Browser. However, if you have no need to run jobs on the agent data of a client computer, you may want to delete the agent that resides on that computer. Once you have uninstalled or DeConfigured the agent, the corresponding icon in the CommCell Browser is grayed out. While this icon exists, you can recover data from the agent to another client. If you delete this icon, all of the agent's data is irretrievably lost.

NOTES

- You cannot delete an agent while operations for that agent are running.
- NAS clients do not use this procedure; for NAS, see Uninstalling Components.

Deleting the agent is a two-phase process.

- You need to uninstall or DeConfigure the agent software from the client computer. Doing so frees an agent license, thereby allowing you to install it on some other computer whose data you do want to secure.
- 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.

Required Capability: See Capabilities and Permitted Actions

To delete an agent:

1. From the CommCell Browser, right-click the icon of the agent that you want to delete, and then click **Delete**. (The agent software must first have been uninstalled/DeConfigured or the delete option on the shortcut menu will not appear.)

2. A warning message prompts you with the following: `This operation will permanently delete the data backed up from this level and it cannot be restored`. Click **Ok** to continue with the deletion operation. (Clicking **No** will abort the operation.)

3. From the **Confirmation Text** dialog box, enter the confirmation text string, `erase and reuse media`. Click **Ok**. The agent icon and the data that corresponds to the selected agent will be deleted. Consequently, you will not be able to browse or recover this data.

VIEW THE SOFTWARE VERSION

To view the Software Version:

1. From the CommCell Browser, click the **CommServe**, **Client**, **Agent**, **MediaAgent**, or **Enabler** for which you wish to view the version, and then click **Properties**.

2. Click the Version tab.

   The component version and post release service pack, additional updates and missing updates are displayed.

CONFIGURE STUB RULE

To configure stub rules for this Agent:

1. From the CommCell Browser, right-click the appropriate agent icon and then click **Properties**.

2. From the Stub Rule tab of the agent Properties dialog box, select the **Preserve stubs until the media has been pruned** radio button to allow stubs to exist until the media retention time has been met and data aging has been run.

3. Optionally select the **Prune stub only after *n* days** radio button and select a value corresponding to the number of days that will determine the minimum life of a stub.

4. Click **OK**.

Archive Sets - SharePoint Archiver Agent

Topics | How To | Related Topics

Overview

SharePoint Archiver Agent Configurable Properties

- Backup Set/Archive Set Name
- User Security

OVERVIEW

After installation of the SharePoint Archiver Agent, the system automatically creates a default archive set.   User-defined archive sets are supported.

See Backup Sets and Archive Sets for information on the different types of archive sets.

SHAREPOINT ARCHIVER AGENT CONFIGURABLE PROPERTIES

Once installed, the agent is configured and is therefore able to manage the data on the client computer. However, you can change certain aspects of the archive set configuration to manage the data in the manner that best suits your needs. You can view or change the archive set configuration from the **Archive Set Properties** dialog box.

The following information can be configured for the SharePoint Archiver Agent:

BACKUP SET/ARCHIVE SET NAME

You can rename a backup set or archive set. For step-by-step instructions, see Rename a Backup Set/Archive Set.

USER SECURITY

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.

For more information, see User Administration and Security.

Archive Sets - SharePoint Archiver Agent - How To

Topics | How To | Related Topics

Change Default Backup Set/Archive Set Designation

Create Backup Sets/Archive Sets

Configure a Backup Set/Archive Set

Associate a Subclient to a Storage Policy

Change Account for Executing Pre/Post Commands (Data Protection)

Rename a Backup Set/Archive Set

Delete a User-Defined Backup Set/Archive Set

CHANGE DEFAULT BACKUP SET/ARCHIVE SET DESIGNATION

Required Capability: See Capabilities and Permitted Actions

► To change the default backup set or archive set designation:

1. From the CommCell Browser, right-click the icon for any supported backup set or archive set that is not currently the default and then click **Properties**.

2. From the **General** tab of the Backup Set/Archive Set Properties dialog box, select the appropriate option to **Make this the default backup set** or **Make this the default archive set**.

3. Click **OK** to save your settings.

CREATE BACKUP SETS/ARCHIVE SETS

Required Capability: See Capabilities and Permitted Actions

To create backup sets/archive sets for the client computer:

1. From the CommCell Browser, locate the correct client computer node, right-click the *i*DataAgent, Agent or instance node (depending on your agent's functionality) for which you want the backup set/archive set created, select **All Tasks** and then click **Create New Backup Set** or **Create New Archive Set**.

2. For most agents, from the **Create New Backup Set** or **Create New Archive Set** dialog box, enter a **New Backup Set Name** or **New Archive Set Name** (up to 32 characters) of the backup set/archive set that you want to create. For the DB2 or DB2 DPF *i*DataAgent, from the same dialog box, click the desired database (backup set) name under **Available DB Name**s and move this name under **Selection**.

   NOTES

   ○ For DB2 or DB2 DPF, to prevent archive log backup failures, ensure that the name that you select is the actual name of the database and not the alias name for the database. If the database name and the corresponding alias name are different, both names are displayed under **Available DB Names**; if both names are the same, the name that is displayed is the database name. To find out about database names and their aliases, run the following command as a DB2 or DB2 DPF instance owner on the DB2 or DB2 DPF client: **db2 list db directory**.

3. Where applicable, if you want to designate this backup set/archive set as the default backup set/archive set, select **Make this the Default backup set** or **Make this the Default Archive Set**; otherwise, leave the check box cleared.

4. For most agents, verify that the storage policy copy associated with the default subclient is the storage policy that you want. If you want to select a different storage policy, click the storage policy box and select the one you want from the list. If the agent supports a system-state subclient, repeat this step for that subclient. For the DB2 or DB2 DPF *i*DataAgent, to establish a storage policy for all the log files, click the storage policy in the list provided.

5. Where applicable, if you want to create additional subclients within this backup set/archive set:

   ○ Click **Add.**

   ○ Follow Create a New Subclient procedure.

   ○ Repeat this step for each additional subclient that you want to define within this backup set/archive set.

   ○ When all subclients have been added, click **OK**.

   ○ A message will advise you to schedule backups for your new backup set. It is recommended that you elect to set a schedule now. You can also associate this backup set/archive set with an All Agent Types schedule policy (which is automatically created by the system, or can be a user-defined Data Protection schedule policy). If you have already associated a schedule policy at a previous level (Agent, Client, or Client Computer Group) the schedules defined in the Schedule Policy will be automatically applied to the new backup set/archive set. See Schedule Policy for more information.

     ■ If you want to associate this backup set/archive set with an All Agent Types schedule policy, click **Associate with Generic Schedule Policy**, and then select that schedule policy from the drop-down list box. Click **OK**.

     ■ If you have selected to define a schedule for this backup set/archive set:

       ■ Click **Schedule**.

       ■ If applicable, from the **Backup Options** dialog box, select the type of backup that you want to schedule.

       ■ If you want to set **Advanced Backup/Archive Options**, click **Advanced**.

       ■ After selecting the backup type and any advanced options, click **OK**. The **Schedule Details** dialog box appears.

       ■ From the Schedule Details tab, select the scheduling options that you want to apply, then click **OK**.

     ■ If you don't want to create a backup/archive schedule at this time, click **Do Not Schedule,** and then click **OK**.

   The new backup set/archive set is displayed in the CommCell Browser.

   A content example for NetWare File System is **SYS:\public**, and an example for NDS content is **OU=prospects.O=engineering.[Root]**.

CONFIGURE A BACKUP SET/ARCHIVE SET

Required Capability: See Capabilities and Permitted Actions

To change the configuration of a backup set, archive set or SQL Server *i*DataAgent database:

1. From the CommCell Browser, right-click the backup set or archive set whose configuration you want to change, and then click **Properties** from the

shortcut menu.

2. From the **General** tab, change one or more of the following fields as appropriate for your agent:
   - **Backup Set Name** - The field accepts 32 characters.
   - **Archive Set Name** - The field accepts 32 characters.
   - **Storage Policy for All Log Files**
   - **User Account -** For the DB2 or DB2 DPF *i*DataAgent, you can add/modify an application/database user account. See the DB2 *i*DataAgents section in **User Accounts and Passwords** for more information.
   - **Make this the default Backup Set** - When selected and committed, this option will make this the default backup set on this client computer.
   - **Make this the default Archive Set** - When selected and committed, this option will make this the default archive set on this client computer.
   - **Use Change Journal** (Recommended) or Use Classic File Scan which includes (**Check archive bit during backups** and/or **Preserve File Access Time**) settings which determine the way subclients within the backup set conduct incremental and differential backups (For an explanation of this field, see Setting the Archive Bit Attribute.)
   - **Use Data Classification** - Specifies that the Data Classification scan is used to determine whether files have been modified for all subclients within the backup set.
   - Select to have data on compressed volumes decompressed before being sent to the backup media. See Decompress Data before Backup for more information. (NetWare File System only.)

3. If your agent uses the Backup tab, click **Edit Rules** for the appropriate subclient type. You can elect to have the system automatically convert the type of backup under the listed conditions. Click **OK** to save your backup rules configuration changes. Without setting this option, if one of these conditions exists your backup will not take place. Subclient Backup Conversion Rules are defined for default subclients and for SQL Server file/file group subclients.

4. Click **OK**.

   - **Exchange Mailbox**

     If you disable the auto-discovery feature, newly created mailboxes will not be backed up unless they are manually discovered and assigned to a subclient.

ASSOCIATE A SUBCLIENT TO A STORAGE POLICY

Required Capability: See Capabilities and Permitted Actions

To associate a subclient to a storage policy:

1. From the CommCell Browser, right-click the subclient whose associated storage policy you want to change, then click **Properties** from the shortcut menu.

2. Click the Storage Device tab of the Subclient Properties dialog box.

3. From the **Storage Policy** list of the **Data Storage Policy** tab, select a data storage policy to associate with this subclient. If necessary, click the **Create Storage Policy** button to create a new storage policy to which the subclient can then be associated.

4. From the Changing a Storage Policy window select the next type of backup operation. Click **OK**.

5. If applicable for your agent, you can change the number of data streams from the **Number of Data/Database Backup Streams** field.

6. If applicable for your agent, click the **Log Storage Policy** tab and select a storage policy to associate with this transaction log subclient from the **Transaction Log Storage Policy** list. Also, you can set the **Number of Transaction Log Backup Streams** from this tab.

7. Click **OK** to save your changes and close the Subclient Properties Storage Device tab.

CHANGE ACCOUNT FOR EXECUTING PRE/POST COMMANDS (DATA PROTECTION)

Required Capability: See Capabilities and Permitted Actions

To change a user account for executing pre/post commands for Data Protection jobs:

1. From the CommCell Browser, expand the tree to view the appropriate level icon for the affected agent.
   - From the agent, instance/partition, or backup set/archive set level, right-click the appropriate icon, click **All Tasks**, and click **New Subclient** from the short-cut menu.
   - From the subclient level, right-click the subclient icon and click **Properties** from the short-cut menu.

2. From the Subclient Properties dialog box, create and/or configure the subclient as appropriate. Then click the **Pre/Post Process** tab.

3. From the **Pre/Post Process** tab, click **Change**.

4. From the User Account dialog box, select one of the account options. If you select **Impersonate User**, type the appropriate user name and password.

5. Click **OK** to save the settings.

RENAME A BACKUP SET/ARCHIVE SET

Required Capability: See Capabilities and Permitted Actions

▶ To rename a backup set or archive set:

1. From the CommCell Browser, right-click the icon for the appropriate backup set or archive set and then click **Properties**.

2. From the **General** tab of the Backup Set/Archive Set Properties dialog box, type the desired name in the **Backup Set** or **Archive Set** field.

3. If you want to make this renamed backup set/archive set the default backup set/archive set, select the corresponding check box (where applicable).

4. Click **OK** to save your settings.

DELETE A USER-DEFINED BACKUP SET/ARCHIVE SET

Before You Begin

● Each agent that utilizes backup sets/archive sets requires the default backup set/archive set in its configuration; therefore, you cannot delete a default backup set/archive set using this procedure. If you want to delete a default backup set/archive set, you must uninstall the agent software that contains it.

● The system does not allow you to delete a backup set/archive set if one of its subclients is being backed up/archived. Any attempt to delete a backup set/archive set under such a condition causes the deletion to fail. If a data protection operation is in progress, do one of the following:

  ○ Wait for the data protection job to complete.

  ○ Kill the data Protection job using the Job Manager.

● When you delete a backup set/archive set, several actions occur:

  ○ The backup set/archive set, its corresponding subclients, and any data that may have been backed up/archived from the backup set/archive set are logically deleted. Once the backup set/archive set is deleted, you can no longer access the corresponding data for restore/recovery purposes.

  ○ All job schedules and job histories that pertain to the subclients of the deleted backup set/archive set are deleted.

Required Capability: See Capabilities and Permitted Actions

▶ To delete a user-defined backup set or archive set:

1. From the CommCell Browser, right-click the user-defined backup set/archive set that you want to delete, select **All Tasks** and then click **Delete**.

2. A confirmation message is displayed, asking if you want to delete the backup set/archive set with all of its subclients. Click **Yes** to continue the deletion, or click **No** to cancel the deletion and retain the backup set.

3. If you clicked **Yes** in the previous step, then the **Enter Confirmation Text** dialog will appear, indicating that all the data in the backup set/archive set will be permanently removed. To confirm this action and continue with the deletion, type `erase and reuse media` in the entry space provided on this dialog. Click **OK**. The system will delete the selected backup set/archive node, the subclient nodes contained within it, and remove them from the CommCell Browser along with any associated data.

Subclients - SharePoint Archiver Agent

Topics | How To | Related Topics

Overview

Subclient Content

Configurable Properties

Things to Consider when Creating and Configuring Subclients

- Common
- SharePoint Archiver

OVERVIEW

The following table shows subclient creation and configuration details.

AGENT	Type of Data	Default Subclient created during install of the Agent	Supports Default Subclient	Supports User Defined Subclient	Contents of the default subclient when user-defined subclient is present	Other Types of subclients supported by the Agent	Notes
SharePoint Archiver	SharePoint Documents	No	No	Yes	N/A	None	None

The following figure shows a simple subclient configuration for a Migration Archiver Agent. Subclient1 and Subclient2 each comprise a unique subset of data on the client computer. Each subclient, when it is archived, establishes a logical data channel through which data can travel to the storage media.
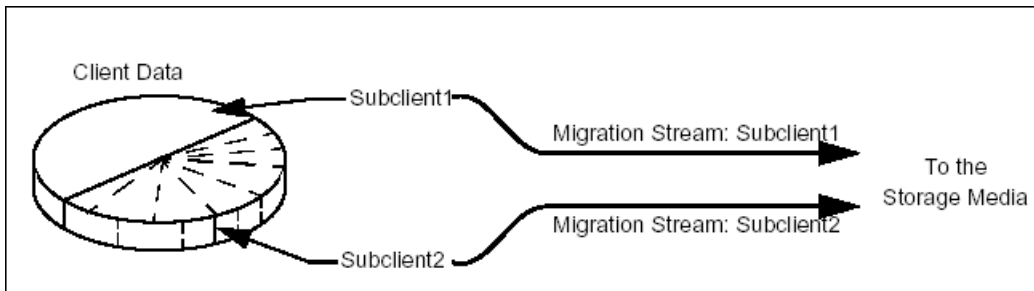
In this configuration, you can schedule archive operations for Subclient1 and Subclient2 either at different times or simultaneously. Splitting the archive operations into two time periods can be useful if you have smaller operation windows at various times.

SUBCLIENT CONTENT

The SharePoint Archiver agent is designed to archive and recover Documents and Images in Document and Picture Libraries residing on an SharePoint Server. The SharePoint Archiver archives all Documents and Images that meet the specified Archiving Rules criteria. Subclient content for this agent consists of Virtual Servers, Sites, and Document and Picture Libraries. After installing this agent, you need to create one or more user-defined subclients.

When you configure subclient content, you select either the Virtual Servers, Sites, Document, Picture Libraries or Library folder you want scanned for archiving. The resulting content will display the URL names similar to the example shown below:

`http://sp-edu/\http://sp-edu\http://sp-edu/graphs\Test Graphs`

A useful way to distribute subclient content of a data type is by Site Collection location, as shown in this example:

- User-defined subclient: subsite Training
  Content: `http://sp-edu/\http://sp-edu\http://sp-edu/Training`
- User-defined subclient: Lib Course Documents
  Content: `https://www.galaxysecure.com/`
  `\https://www.galaxysecure.com/sites/southeast\https://www.galaxysecure.com/sites/southeast/docs\Course Documents`

Distributing the client data using subclients in this way can help improve archiving performance in cases where your site manages a high volume of SharePoint data.

FILTERING

Subclient-level Archiving Filters are available for this agent to exclude specified Virtual Servers, Sites, and Document and Picture Libraries from being scanned for archiving. For example, suppose the Site contains a subfolder called `Obsoleted Projects` that you do not want backed up. You can add a Subclient Filter for the user-defined subclient `Event Planning` to exclude the `Obsoleted Projects` subfolder from being scanned for archiving. For more information, see Filters.

WILDCARDS AND REGULAR EXPRESSIONS

Wildcards and regular expressions are not supported for this agent when defining Subclient Content or Filters.

CONSIDERATIONS

For more information, see Things to Consider when Creating and Configuring Migration Archiver Subclients.

CONFIGURABLE PROPERTIES

Once installed, the agent is configured and is therefore able to manage the data or volumes on the client computer. However, you can change certain aspects of the subclient configuration to manage the data in the manner that best suits your needs.

You can view or change the subclient configuration from the Subclient Properties dialog box. The following information can be configured.

ACTIVITY CONTROL

You can enable or disable all operations for this CommCell object and all objects below it. For more information, see Activity Control.

ARCHIVING RULES

You can establish the criteria for a Migration Archiver subclient to determine which content will be scanned (i.e., mailboxes, libraries, volumes, folders, and directories) and which data objects will be archived (i.e., messages, items, and files). You can also establish stub creation rules, set the interval at which a new index is created and other related criteria.

For more information, see Subclient Properties (Archiving Rules).

CONTENT/DATABASES

You can define the content of the subclient. Most agents include a configure button that displays a dialog where you can add or modify the data included as subclient content. For step-by-step instructions, see Configure Subclient Content.

For more information, see Subclient Content.

DATA TRANSFER OPTIONS

Several configurable options to efficiently use available resources for transferring data secured by data protection operations are provided in the subclient. 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.

DATA ENCRYPTION

You can enable or disable the encryption of data for transmission over unsecure networks and for storage on media. For more information, see Data Encryption.

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 for the subclient including their priority. For additional information, see Configuring Alternate Data Paths for Subclients.

DATA PROTECTION FILTERS

You can perform the following functions:

- Define data protection filters to exclude specified subclient data from being backed up or archived. For more information, see Filters.
- Use regular expressions (or wildcards) in subclient data protection exclusion filters. See Inclusions, Exclusions, and Exceptions to Exclusions for more information.
- Perform in-place editing of subclient data protection filter exclusions and exceptions. See Editing Filters for more information.

DEDUPLICATION

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. For more information, see Deduplication.

PRE/POST PROCESSES

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. For more information, see Pre/Post Processes.

STORAGE POLICIES

You can associate the subclient to a storage policy. For more information, see Storage Policies.

SUBCLIENT NAME

You can rename a user-defined subclient.

USER ACCOUNTS

You can define an account with permissions to execute Pre/Post commands for the agent's archive, backup, or volume creation jobs.

See SharePoint Agents in **User Accounts and Passwords** for more information.

USER SECURITY

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.

For more information, see User Administration and Security.

THINGS TO CONSIDER WHEN CREATING AND CONFIGURING SUBCLIENTS

When creating and configuring subclients, keep in mind the following considerations:

COMMON

- When creating and configuring a subclient, you will need to establish the archiving rules for the subclient, in addition to specifying the subclient name, storage policy association and content.

- If you enable the Do Not Create Stub or Archive Files Only, Do Not Create a Stub archiving rule option, a non-browse recovery operation is not possible and archived data must be recovered via the browse/recovery operation from the CommCell Console.

- For archive filter considerations, see Archive Filters for Migration Archiver Agents.

SHAREPOINT ARCHIVER

- Subclient content is defined up to the library folder level.

- After creating a subclient, you must clear the **Disable All Rules** option and configure archiving rules before Archive Operations are possible. Otherwise, the system will ignore all archiving rules (except for the Do Not Create Stub rule) for the subclient.

Back to Top

Subclients - SharePoint Archiver Agent- How To

Topics | How To | Related Topics

Common

Add a Data Protection Filter for a Subclient

Associate a Subclient to a Storage Policy

Associate or Disassociate a User Group to a Subclient

Change Account for Executing Pre/Post Commands (Data Protection) (Windows-based agents)

Configure a Subclient for Pre/Post Processing of Data Protection Operations

Configure Subclient Content

Configure the Subclient for Data Encryption

Create a New Subclient

Delete a Data Protection Filter from a Subclient

Delete a User-Defined Subclient

Enable or Disable Operations

Enable or Disable Software Compression for a Subclient

Remove a Process from Pre/Post Processing of Data Protection Operations

Rename a Subclient

Set the Network Bandwidth and Network Agents for a Data Protection Operation

View Data Paths Associated with a Subclient

View Subclient Content

ADD/EDIT A DATA PROTECTION FILTER FOR A SUBCLIENT

Before You Begin

- Review Filters.

- Do not change the data protection or discovery filter of a subclient that has a data protection operation in progress.

- The system does not allow you to add entries that are not content of a particular subclient to that subclient's filter.

- For BlueArc and EMC Celerra (running at least DART OS 5.6.x) subclients, the filter string with or without wildcards must match the name or path of the file or directory being filtered.

- For NetApp subclients only name type filters (with wildcards) are supported:
  - You cannot enter paths as a filter (e.g. /vol/vol0/data1). Since NetApp does not support the use of paths in filters, if there are multiple files with the same name, even though they may be in different directories, all of them will be excluded from backups.
  - Name of the file or directory must exactly match the filter string.
  - You can specify a maximum of 32 strings in the exclude list.

Select the desired procedure:

- To add a data protection or discovery filter for a subclient

- To edit a data protection filter for a subclient

Required Capability: Capabilities and Permitted Actions

To add a data protection or discovery filter entry for a subclient:

1. From the CommCell Browser, right-click the subclient whose data protection or discovery filter you want to add, and then click **Properties** from the shortcut menu.

2. Click the Filters tab of the Subclient Properties dialog box.

3. For Exchange Mailbox, Exchange Mailbox/Public Folder Archiver Agents and Exchange Compliance Archiver, to specify a mailbox or folder that you want to exclude from data protection operations:
   - Click the upper **Add** button.
   - From the Browse window, expand the mailbox tree of the client computer.
   - Click the mailbox or folder that you want to exclude from the backup/archive operations on the selected subclient, and then click **Add**. (Repeat this step for each additional entry.)
   - From the Browse window, click **OK**.

   The mailboxes or folders that you selected appear as entries in the upper pane. Repeat this step if you want to add more mailboxes and/or folders to the filter.

4. For NAS NDMP *i*DataAgents, click the **Add** button and, in the input window, type the name of the file, directory, (or path for BlueArc) that you want to exclude from the backups and click **OK**. The name displays as an entry in the **Exclude these files/folders/patterns** pane. Repeat this step if you want to add more files, directories, or paths to the filter.

5. For SharePoint Server *i*DataAgents, to specify a URL/file/folder/pattern that you want to exclude from data protection operations or to specify an exception filter for database backup sets, do one of the following:

- Click the **Add** button next to **Exclude these files/folder/patterns**: input window and type the URLs of site collections that you want to exclude from the backups and click **OK**. The site collection displays as an entry in the **Exclude these files/folders/patterns** pane. Wildcards are supported. See Wildcards for more information. Repeat this step if you want to add more URLs, files, directories, or paths to the filter.
- Click the **Add** button next to **Except for these files/folders**: input window and type the URLs/folders of site collections that you want to be exceptions for the exclusion filter and click **OK**. These exceptions will be included in the data protection operations. Wildcards are not supported for exception filters.

6. For Exchange Public Folder *i*DataAgents and SharePoint Server *i*DataAgent, to specify a workspace/folder that you want to exclude from the backups, click the upper **Browse** button and expand the *i*DataAgent of the client computer. Click the workspace/folder that you want to exclude from the backups and then click **Add**. Repeat this step for each additional entry.

7. For Windows/Unix/Macintosh File System *i*DataAgents, File Archiver for Windows/Unix Agents, and ProxyHost *i*DataAgent, to specify a file/folder/directory that you want to exclude from data protection operations, do one of the following:
   - Click the upper **Add** button and, in the **Enter Path** window, type the complete path (including drive letter) of the file/folder/directory that you want to exclude from the backups/archive operations. Repeat this step if you want to add more files/folders/directories to the filter.
   - Click the upper **Browse** button and expand the file system of the client computer. Click the file/folder/directory that you want to exclude from backups/archive operations and then click **Add**. Repeat this step for each additional entry.

8. For NetWare File System/NDS *i*DataAgents, to specify data that you want excluded from the backups, do one of the following:
   - To manually enter the path:
     - Click the **Add** button.
     - In the Input window, type the complete path (e.g., VOL1:\demo\disk2) of the data that you want to exclude.
     - Click **OK**. (The path that you typed displays as an entry in the upper pane.) Repeat this step if you want to exclude more data.
   - To browse and select a path:
     - Click the **Browse** button.
     - From the Backup Data window, expand the file system or NDS tree of the NetWare server.
     - Select the data that you want to exclude, and then click **Add**. Repeat this step for each additional entry.
     - From the Backup Data window, click **OK.** The data that you selected displays as entries in the upper pane.

9. For Lotus Notes Database and Lotus Notes Document *i*DataAgents, to specify a file or folder that you want to exclude from discovery, do one of the following:
   - Select the **Pattern/path to be excluded** field. Then type in a file or folder that you want to exclude. The format of the entry should start with a slash (\). The path entered is always relative to the data path of the partition. Then click **Add**. Repeat this step for each additional entry.
   - Click the upper **Browse** button and expand the file system of the client computer. Click the file or folder that you want to exclude from the backups and then click **Add**. Repeat this step for each additional entry.

10. For Exchange Mailbox, Exchange Mailbox/Public Folder Archiver Agents and Exchange Compliance Archiver, to specify a wildcard pattern of the folders that you want to exclude across all mailboxes within the subclient:
    - Click the lower **Add** button.
    - In the Input window, type the wildcard pattern of the folders that you want to exclude from backup/archive operations on the selected subclient.
    - Click **OK**. The path that you typed appears as an entry in the lower pane. Repeat this step if you want to add more entries to the filter.

11. For Exchange Public Folder *i*DataAgents and SharePoint Server *i*DataAgent, to specify an exception to an excluded workspace/folder (i.e., a folder/document that you want included in the backups, but whose parent directory has been excluded), click the lower **Browse** button and expand the *i*DataAgent of the client computer. Click the workspace/folder that you want to include in the backups and then click **Add**. Repeat this step for each additional entry.

12. For Windows/Unix/Macintosh File System *i*DataAgents, File Archiver for Windows/Unix Agents, and ProxyHost *i*DataAgent, to specify an exception to an excluded folder/directory (i.e., a file or folder/directory that you want included in the data protection operations, but whose parent folder/directory has been excluded), do one of the following:
    - Click the lower **Add** button and, in the **Enter Path** window, type the complete path (including drive letter) of the file/folder/directory that you want to include in the backups/archive operations. Repeat this step if you want to add more exceptions to the filter.
    - Click the lower **Browse** button and expand the file system of the client computer. Click the file/folder/directory that you want to include in the backups/archive operations and then click **Add**. Repeat this step for each additional entry.

13. For NetWare File System/NDS *i*DataAgents, to specify an exception to an excluded directory or NDS container (i.e., data that you want included in the backups, but whose parent directory or NDS container has been excluded), do one of the following:
    - To manually enter the path:
      - Click the **Add** button.
      - In the Input window, type the complete path (e.g., VOL1:\demo\disk2\readme) of the data that you want to include.
      - Click **OK**.
    - To browse and select a path:

- Click the **Browse** button.
- From the Backup Data window, expand the file system or NDS tree of the NetWare server.
- Click the file or folder that you want to include in the backups and then click **Add**. Repeat this step for each additional entry.
- Click **OK.** The selected data displays as entries in the lower pane.

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

Required Capability: Capabilities and Permitted Actions

To edit a data protection filter entry for a subclient:

1. From the CommCell Browser, right-click the subclient whose data protection filter you want to edit, and then click **Properties** from the shortcut menu.

2. Click the Filters tab of the Subclient Properties dialog box.

3. Click the filter entry that you want to edit, and then click the **Edit** button associated with that pane.

4. Type the changes into the **Enter Path** dialog box, then click **OK**.

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

NOTES

- When you change a data protection or discovery filter, the change is effective the next time a data protection operation is run on the applicable subclient.
- Performing a full backup after changing filters or exceptions is recommended.

ASSOCIATE A SUBCLIENT TO A STORAGE POLICY

Required Capability: See Capabilities and Permitted Actions

To associate a subclient to a storage policy:

1. From the CommCell Browser, right-click the subclient whose associated storage policy you want to change, then click **Properties** from the shortcut menu.

2. Click the Storage Device tab of the Subclient Properties dialog box.

3. From the **Storage Policy** list of the **Data Storage Policy** tab, select a data storage policy to associate with this subclient. If necessary, click the **Create Storage Policy** button to create a new storage policy to which the subclient can then be associated.

4. From the Changing a Storage Policy window select the next type of backup operation. Click **OK**.

5. If applicable for your agent, you can change the number of data streams from the **Number of Data/Database Backup Streams** field.

6. If applicable for your agent, click the **Log Storage Policy** tab and select a storage policy to associate with this transaction log subclient from the **Transaction Log Storage Policy** list. Also, you can set the **Number of Transaction Log Backup Streams** from this tab.

7. Click **OK** to save your changes and close the Subclient Properties Storage Device tab.

ASSOCIATE OR DISASSOCIATE A USER GROUP TO A COMMCELL OBJECT

Required Capability: See Capabilities and Permitted Actions

To associate or disassociate a user group to a CommCell entity:

1. From the CommCell Browser, click the CommServe, client computer group, client computer, agent, MediaAgent, Library, Storage Policy, backup set, subclient, or Shelf media, and then select **Properties**.

2. From the **Security** tab, 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.

3. Click **OK**.

CHANGE ACCOUNT FOR EXECUTING PRE/POST COMMANDS (DATA PROTECTION)

Required Capability: See Capabilities and Permitted Actions

To change a user account for executing pre/post commands for Data Protection jobs:

1. From the CommCell Browser, expand the tree to view the appropriate level icon for the affected agent.

   ○ From the agent, instance/partition, or backup set/archive set level, right-click the appropriate icon, click **All Tasks**, and click **New Subclient** from the short-cut menu.

○ From the subclient level, right-click the subclient icon and click **Properties** from the short-cut menu.

2. From the Subclient Properties dialog box, create and/or configure the subclient as appropriate. Then click the **Pre/Post Process** tab.

3. From the **Pre/Post Process** tab, click **Change**.

4. From the User Account dialog box, select one of the account options. If you select **Impersonate User**, type the appropriate user name and password.

5. Click **OK** to save the settings.

CONFIGURE A SUBCLIENT FOR PRE/POST PROCESSING OF DATA PROTECTION/ARCHIVE OPERATIONS

Before You Begin

● We recommend not configuring a pre/post process for a subclient that is currently running a data protection or archive operation.

● Verify that there are no pre/post processes already assigned for the subclient.

● Review the Overview and Agent-Specific Guidelines for your agent before configuring pre/post processes for data protection/archive operations.

● Pre-process commands for the *i*DataAgents will be executed only when the necessary resources (e.g., media, library, drive, etc.) are available.

Required Capability: Capabilities and Permitted Actions

► To configure a subclient for Pre/Post processing of data protection/archive operations:

1. From the CommCell Browser, right-click the subclient for which you want to configure a pre/post process, and then click **Properties** from the shortcut menu.

2. Click the Pre/Post Process tab of the Properties dialog box.

3. For an agent other than the Oracle RAC *i*DataAgent, click inside the space that corresponds to one of the following phases and type the full path of the process that you want executed during that phase. Alternatively, click **Browse** to locate the process (applicable only for paths that do not contain any spaces). For the Oracle RAC *i*DataAgent, click **Browse** for the corresponding process, click the name of the control node client in the Select Client for Browse dialog box, and click **OK**. Then browse for and click the process.

   ○ PreBackup
   ○ PreScan
   ○ PreArchive
   ○ PreCopy
   ○ PreSnap
   ○ PostBackup
   ○ PostScan
   ○ PostArchive
   ○ PostCopy
   ○ PostSnap

   Click **OK**.

4. If you want to run a Post Process for all attempts to run that job phase, then select the corresponding checkbox.

5. For subclients on Windows platforms, if **Run As** displays **Not Selected**, or 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 a 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.

6. Click **OK** to save your changes and close the Pre/Post Process tab of the Properties dialog box.

CONFIGURE ARCHIVING RULES - SHAREPOINT ARCHIVER AGENT

Related Topics:

● Archiving Rules

Before You Begin

● Do not change the archiving rules of a subclient that is being archived.

Required Capability: Capabilities and Permitted Actions

► To configure archiving rules for the SharePoint Archiver Agent:

1. From the CommCell Browser, right-click the subclient whose archiving rules you want to configure, then click **Properties** from the shortcut menu.

2. Click the Archiving Rules tab of the Subclient Properties dialog box.

3. Clear the **Enable all rules** checkbox to disable rules-based migration archiving operations for this subclient. When this option is selected, all archiving rules will be ignored except for Stub Management rules. If you select this option, then go to Step 7, otherwise, for rules-based migration archiving operation, continue to the next step.

4. On the Document Rule tab:
   ○ In the **Archive documents whose Modified Time is older than the specified days** field, enter or select a value corresponding to the number of days elapsed since the last Modified Time of each document, in order for the document to be archived.
   ○ In the **Archive documents whose Size is greater than a specified threshold** field, enter or select a value corresponding to the size (in Kilobytes) a document must be in order for the document to be archived.
   ○ In the **Archive versions older than the last specified versions** field, enter or select a value corresponding to the number of versions that will be subtracted from the current version in order to archive the document.
   ○ You can optionally select the **Archive if: All of the above rules are satisfied** checkbox to archive a document if it satisfies ALL of the general criteria established above.
   ○ You can optionally select the **Archive if: Any of the above rules are satisfied** checkbox to archive a document if it satisfies one or more of the general criteria established above.

5. On the User tab:
   ○ You can **Add**, **Delete** or **Browse** SharePoint users for the **Archive documents whose owner is listed below** list to configure documents to be archived based on user ownership. This criteria is used in conjunction with the General and Type criteria to determine whether documents will be archived.
   ○ You can **Add**, **Delete** or **Browse** SharePoint site groups for the **Archive documents whose owner belongs to one of the site groups listed below** list to configure documents to be archived based on site group ownership. This criteria is used in conjunction with the General and Type criteria to determine whether documents will be archived.

6. On the Type tab, you can **Add** or **Delete** document types in the **Archive documents whose type is listed below** list to configure documents to be archived based on type. This criteria is used in conjunction with the General and Type criteria to determine whether documents will be archived. This criteria is used in conjunction with the General and Type criteria to determine whether documents will be archived.

7. On the Stub Rule tab, you can:
   ○ Optionally select the **Do not create stub** checkbox so that no stubs are created for archived documents.

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

CONFIGURE SUBCLIENT CONTENT

Before You Begin

● Review Subclients.

● Do not configure the content of a subclient while the parent node or any sibling subclient has a data protection or archive operation currently running on it.

● Exchange Mailbox *i*DataAgents and Exchange Mailbox/Public Folder Archiver Agents: If you change the contents of the default backup set or archive set then the auto-discover feature will be disabled. If you disable the auto-discovery feature, newly created mailboxes will not be backed up/archived unless they are manually discovered and assigned to a subclient.

● NAS NDMP *i*DataAgents: You must ensure there is no overlap in content between all subclients. Overlap in subclient content will result in loss of data. An existing subclient's contents are not automatically changed when another subclient is added with overlapping contents.

● SharePoint Server *i*DataAgent: The Site Content Database, the Site Collection Database, the Site Database, and the Site Index for the virtual server must all be assigned to the same subclient.

● Lotus Notes Document *i*DataAgent: Review Assigning Restore View Names to Newly-discovered Databases

● QR Agent: Follow these guidelines when adding a volume to a QR Agent subclient:
   ○ The volume must correspond to a physical disk or RAID array.
   ○ A volume created by volume management software other than VxVM is not valid subclient content.
   ○ Subclients may have overlapping content; however, if two or more subclients overlap, they all must use the same snapshot engine. If the QR policies associated with the subclients are configured to use different snap engines, they must be reconfigured to use the same snap engine in this scenario.

● **Caution Against Re-configuring Default Subclient Content**

   We recommend that you do not re-configure the content of a default subclient because this would disable its capability to serve as "catch-all" entity for client data. As a result, the likelihood that some data will not get backed up or scanned for archiving would increase.

Required Capability: See Capabilities and Permitted Actions

► To configure subclient content:

1. From the CommCell Browser, right-click the subclient for which you want to configure content, click **All Tasks** (if applicable) and then click **Properties**.

2. Follow the procedure below that is applicable for your agent:

   ○ For File System, Active Directory, File Archiver, Exchange Public Folder *i*DataAgents, NDS, and SharePoint Server *i*DataAgents click the Subclient Properties (Content) tab and configure content for the subclient as described below for your agent:

     ■ For File System, Active Directory, File Archiver, NDS, and SharePoint Server *i*DataAgents: Type the full path of the data that you want to include as subclient content in the **Enter New Content** field, then click **Add**. Optionally, click **Browse** to enter the content. When browsing content while configuring SharePoint subclients, you can add content via multiple selections with the CTRL or SHIFT keys. For Windows, when specifying a UNC Path, click **As User**, and enter the user account information for the domain user with permissions for that path. For NetWare/DNS, see the Notes section below for content path examples. For Unix File Systems, you can enter the mount point of an NFS-mounted file system, see the Notes section below for examples.

     ■ For Exchange Public Folder *i*DataAgents: Click **Browse**, select folders to include as content, then click **Add**.

     ■ For the Unix File System *i*DataAgents, to facilitate the management of resource fork data in Apple double-encoded Macintosh files, click **Enable Apple Double Support**.

     ■ For the Unix File System *i*DataAgents, to view the actual data path for any symbolic link in the subclient content, click **Expand symbolic links of subclient content** and then click **Discover**.

   ○ For NAS NDMP *i*DataAgents, configure the **Backup Content Path** field(s) as described below, then click **Add**:

     ■ 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`.

     ■ Optionally, for NetApp NAS NDMP, click **Browse** to enter the content.

   ○ For Exchange Mailbox and Exchange Mailbox/Public Folder Archiver Agents follow the procedure to Discover and Assign New Mailboxes or Assign Mailboxes to Another Subclient.

   ○ For Lotus Notes Database and Document *i*DataAgents follow the procedure to Discover and Assign New Databases or Assign Databases to a Subclient.

   ○ For DB2, DB2 DPF, Exchange Database, Novell GroupWise, SharePoint Server, SQL Server Database, Sybase, and MySQL *i*DataAgents, click the Subclient Properties (Content) tab and configure content for the subclient as described below for your agent:

     ■ For the DB2 *i*DataAgent, specify whether you want to include the entire database or a subset of this data as content for the subclient. For the DB2 DPF *i*DataAgent, specify whether you want to include all the affected database partitions or a subset of this data as content for the subclient.

     ■ For Exchange and GroupWise *i*DataAgents: Click **Configure**. From the Add/Modify Subclients dialog box click the subclient entry for the database element/Storage Group that you want to add to the new subclient and select the name of the destination subclient from the list that appears. Alternatively, you can select and assign a range of databases/storage groups using the **Change all selected databases/storage groups to** list. Note that you must have at least one database element/Storage Group assigned to this subclient in order to save the configuration.

       A database/Storage Group that is not configured for a subclient does not appear in the list. This can be the case if the subclient containing the database/Storage Group was deleted. If this happens, click **Discover** to display all databases/Storage Groups.

     ■ For the SharePoint Server *i*DataAgent, follow the procedure to Discover and Assign New Data Types.

     ■ For the Sybase *i*DataAgent, follow the procedure to Manually Discover Databases.

     ■ For the MySQL *i*DataAgent, follow the procedure to Configure MySQL Databases.

   ○ For the Informix *i*DataAgent, click the Subclient Properties (Content) tab and define the contents of the subclient. Specifically, establish the backup mode for the data to be backed up, set the backup level, and decide whether to back up the emergency boot file and/or the ONCONFIG file.

   ○ For the Oracle, SAP for Oracle, or Oracle RAC *i*DataAgent, click the Subclient Properties (Content) tab and define the contents of the subclient. To configure this subclient for specialized types of backups, follow the appropriate procedure below:

     ■ Create Subclient for Backing Up Archived Redo Log Files

     ■ Create Subclient for Backing Up Offline Databases

     ■ Create Subclient for Backing Up Online Databases

     ■ Create Subclient for Performing Selective Online Full Backups

   ○ For SAN *i*DataAgents, click the Subclient Properties (Content) tab and configure content for the subclient as described below for your agent:

     ■ Image Level on Unix *i*DataAgent: Click **Add**. From the Add Content Path dialog box, select the volume(s) that you want to back up (use CTRL + click to select multiple volumes). Click **OK**. The selected volumes are added to the **Contents of subclient** list. These volumes are automatically

configured to be CXBF devices. Alternatively, use Volume Explorer per specific scenarios to configure CXBF devices.

To configure an unmounted block device or raw device as content, first use Volume Explorer to configure the device as a CXBF device. Then select the configured CXBF device as subclient content. You can ignore the warning that is displayed.

For more information, see When to Use Volume Explorer. For a step-by-step procedure, see Configure a CXBF Device in Volume Explorer.

- Image Level and Image Level ProxyHost on Windows *i*DataAgents: Click **Add**. Then in the **Add Content** dialog box, type the full path of the volume or mount point that you want to include as subclient content, then click **Add**. Optionally, click **Browse** to select the content. Click **OK**. The volume or mount point is added to the **Contents of subclient** list. Add additional content by repeating this step.
- ProxyHost *i*DataAgent: Select a backup host from the **Backup Host** list. This is the computer to which the BCV is connected. Click **Add**. In the **Content** field of the Add/Edit Content for Subclient dialog box, type the primary host path of the content that you want to back up, or click **Browse** to find and select this data. In the **Backup Host BCV Path** field of the Add/Edit Content for Subclient dialog box, type the path through which the backup host accesses this data on the BCV, or click **Browse** to find and select this path. Click **OK**. The primary host data path and corresponding backup host BCV path are added as a single entry in the **Contents of subclient** list. To add additional entries, repeat these steps. Refer to Notes below for more information.

  ○ For Quick Recovery Agents, click the Subclient Properties (Content) tab and configure the following options:

  - Click **Add Volume**. From the Adding Volume dialog box, select volume(s) that you want to add to the subclient content (use CTRL + click to select multiple volumes). You can add/edit additional advanced options for the selected volume by select **Advanced** on the Adding Volume dialog box. Click **OK**.
  - Click Add App to select an application and associated volumes. Click **OK**.

    Any instances you intend to protect and recover with the QR Agent must be configured in the QR Agent properties Authentication tab. They will not appear in the Add App dialog box if they are not configured. Only volumes containing datafiles and archive log files will be detected by Add App. Volumes containing control files and redo log files will not be detected.

    For a clustered Exchange Server, if you are *not* using VSS to perform an online quiesce, sufficient permissions are required in order to be able to perform an offline quiesce; in such cases, ensure that the **User Name** specified has Exchange Administrator rights.

    See also Configure Subclients for Overlapping Content.

3. Click **OK** to save your content configuration.

NOTES

- Content examples for NetWare are **OU=prospects.O=engineering.[Root]**, (for NDS content), and **SYS:\public** (for File System content).
- Content examples for adding an NFS-mounted file system to subclient content of a Unix File System *i*DataAgent:
  ○ */mountpointA* to include the entire file system at mountpointA
  ○ */mountpointA/projects* for only the *projects* directory within the file system at mountpointA.
- Informix subclients include one or more dbspaces. As databases are added to the dbspaces, the subclients are updated automatically.
- Exchange Mailbox *i*DataAgents and Exchange Mailbox/Public Folder Archiver Agents: Initially, all unconfigured mailboxes are assigned to the default subclient. You can create a new subclient and reassign mailboxes to this new subclient (within the same backup set/archive set). Once assigned, the mailboxes become part of the content of the new subclient.
- SharePoint Server *i*DataAgent: Initially, all unconfigured data types are assigned to the default subclient. You can create a new subclient and reassign data types to this new subclient. Once assigned, they become part of the content of the new subclient.
- ProxyHost *i*DataAgent: The primary host data path is backed up by the subclient and is the path through which the backup host accesses this data on the BCV. A primary host path and its corresponding backup host path are listed in the following format:

  <primary_host_path> --> <backup_host_path>

  For example, assume that you want to back up the **D:\data** directory from your primary host and **D:** is mirrored by a BCV, which is mapped to the backup host as **F:**. Consequently, the path to this data on the backup host is **F:\data.** When you add this directory to a subclient, it is listed in the **Contents of subclient** pane as **D:\data --> F:\data**.

  > The primary host path in the **Content** field is used for browse and restore purposes. However, it is the data in the **Backup Host BCV Path** which is actually backed up. If these two paths do not accurately correspond, the path that appears when data is browsed for restore does not accurately reflect the data that will be restored. In the example given above, assume that **D:\data** is entered in the **Content** field, while **F:\data1** is accidentally entered in the **Backup Host BCV Path**. If you browse and select **D:\data** to be restored, it is actually **D:\data1** that is restored. (Remember, **F:\Data1** is the path on the backup host that corresponds to **D:\data1** on the primary host.)

CONFIGURE THE SUBCLIENT FOR DATA ENCRYPTION

Encryption settings made at the subclient level are for data protection and recovery operations run from the CommCell Console and are not related in any way to settings made at the instance level which is for third-party Command Line operations only.

See Data Encryption - Support for a list of supported products.

Before You Begin

- Encryption must be enabled at the client level prior to configuring any subclients residing on that client. See Configure the Client for Data Encryption.

- If you are attempting to configure for third-party Command Line operations, do not use this procedure. See Configure Third-party Command Line Operations for Encryption.

Required Capability: Capabilities and Permitted Actions

To configure the subclient for data encryption:

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

2. From the Subclient Properties (Encryption) tab, select an option based on the criteria described in the Encryption tab help.

3. Click **OK** to save your settings and close subclient properties.

CONFIGURE THE SUBCLIENT FOR DATA ENCRYPTION

Encryption settings made at the subclient level are for data protection and recovery operations run from the CommCell Console and are not related in any way to settings made at the instance level which is for third-party Command Line operations only.

See Data Encryption - Support for a list of supported products.

Before You Begin

- Encryption must be enabled at the client level prior to configuring any subclients residing on that client. See Configure the Client for Data Encryption.

- If you are attempting to configure for third-party Command Line operations, do not use this procedure. See Configure Third-party Command Line Operations for Encryption.

Required Capability: Capabilities and Permitted Actions

To configure the subclient for data encryption:

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

2. From the Subclient Properties (Encryption) tab, select an option based on the criteria described in the Encryption tab help.

3. Click **OK** to save your settings and close subclient properties.

CREATE A NEW SUBCLIENT

Before You Begin

- Review Subclients.

- Do not create a subclient while the parent node or any sibling subclient has a data protection or archive operation currently running on it.

- In cases where a new subclient is created with the same name as a deleted subclient, the system will append a Unix time stamp to the deleted subclient's name in data protection job history reports and views to distinguish the two subclients. For example, *subclientname*_1104257351.

- Informix *i*DataAgents: If you will be using the Informix ONBAR utility to create backup and restore scripts, you need not create subclients. Otherwise, if you will be using the CommCell Console to back up and restore Informix database objects (subsets/dbspaces), then you will need to create a subclient.

- ProxyHost *i*DataAgents: If you are using a BCV, you must prepare a batch file or a shell script file on the backup host containing commands to synchronize and split the BCV. The Resource Pack includes information on configurations for these batch files or shell scripts, as well as examples that apply to specific applications and hardware (e.g., Exchange databases in an EMC Symmetrix environment). See Resource Pack for more information on the Resource Pack.

  The ProxyHost *i*DataAgent also requires that you set permissions for the batch/shell script file on the backup host.

- SQL Server Database *i*DataAgents: When running on Windows Server 2003 and VSS is enabled, the **New Subclient** command is not available.

- PostgreSQL *i*DataAgents: Once you configure the PostgreSQL instance, the system automatically generates the default backup sets and default subclients. However, you can use the CommCell Console to create user-defined subclients for dump backup sets to distribute some of the database content. You cannot create user-defined subclients for FS backup sets.

Required Capability: See Capabilities and Permitted Actions

To create a new subclient:

1. From the CommCell Browser, right-click the node (agent/backup set/archive set/instance) for which you want to create a new subclient, click **All Tasks** (if applicable), and then simply click **New Subclient** for most agents.
   - For the SQL Server *i*DataAgent, expand **New Subclient** and click either **Database** to include individual databases or **File/File Group** to include database elements**.**

2. Click the General tab or General (Quick Recovery Agent) tab of the Subclient Properties dialog box and type the name (up to 32 characters) of the subclient that you want to create.

- For supported agents identified in Support Information - Snapshot Engines, you can select a QSnap option to snap data and then perform a data protection operation on the data.

- For Image Level on Unix and Image Level ProxyHost on Unix, use the **Incremental Support Using** field to configure either a CXBF subclient or a checksum subclient and to enable incremental support for either subclient type.

- For QR Agents, you must also select a QR Policy from the **QR Policy** list.

- For the Windows *i*DataAgents that support VSS, you can optionally Enable VSS on a Subclient.

3. Select other options from the General tab as appropriate for the agent.

4. Click the **Content** or **Databases** tab of the Subclient Properties dialog box and Configure Subclient Content as appropriate for your agent.

5. For all agents (except QR), click the Storage Device (Data Storage Policy) tab of the Subclient Properties dialog box, then select a data storage policy to associate with this subclient from the storage policy list.

- For the DB2 and DB2 DPF *i*DataAgents, you can also change the number of data backup streams. For the DB2 DPF *i*DataAgent, the default stream threshold should be equal to the total number of database partitions for the subclient.

- For SQL Server *i*DataAgents, you can also click the Storage Device (Log Storage Policy) tab of the Subclient Properties dialog box, then select a log storage policy to associate with this subclient from the storage policy list and select the number of backup streams for transaction log backup jobs.

- For 1-Touch for Unix, it is strongly recommended that the storage policy that you select for the subclient configured for 1-Touch use a MediaAgent on a different computer. If you do this, and if the system crashes, the media will not have to be exported to another MediaAgent in order to recover the system.

6. For Oracle and DB2 *i*DataAgents, click the Backup Arguments (Oracle) or Backup Arguments (DB2, DB2 DPF) tab of the Subclient Properties dialog box and Configure Backup Arguments as appropriate for your agent. Note that the backup arguments for Informix are located on the Content tab.

7. For Migration Archiver Agents, click the **Archiving Rules** or **Rules** tab of the Subclient Properties dialog box and configure archiving rules as appropriate for your agent. In order to perform rules-based migration archiving operations, the **Disable All Rules** checkbox must be cleared.

   If the File Archiver for Windows supports Data Classification, several filter-like configuration fields are defined as archiving rules and are available from the Subclient Properties (Rules) tab. If you want to define content and archiving rules based on file attributes other than volumes, size, and modified time (i.e., if you want to customize your rules), click the Advanced tab and configure as appropriate. Also, stub management options can be configured from the Stub Rule tab. See Configure Archiving Rules - File Archiver Agents for step-by-step instructions.

8. For ProxyHost and Image Level ProxyHost *i*DataAgents, click the Pre/Post Process tab of the Subclient Properties dialog box. In the **PreScan** field, type the path to the batch file/shell script file that contains those commands that are to run before each backup of the subclient, or click **Browse** to locate and select this file. For ProxyHost and Image Level ProxyHost, the file must reside on the backup host or primary host.

9. Optionally (if supported for your agent) you can:

   - Add a Data Protection or Discovery Filter for a Subclient on the Filters tab.

   - Configure a Subclient for Pre/Post Processing of Data Protection/Archive Operations on the Pre/Post Process tab.

   - Enable Software Compression for a Subclient on the Software Compression tab of the **Storage Device** tab.

   - Configure the Subclient for Data Encryption on the Encryption tab.

   - Enable or Disable Operations for this subclient on the Activity Control tab.

   - Configure Mailbox Stores for Auto-Discovery on the Auto-discovery tab.

   - Configure the Subclient for 1-Touch on the 1-Touch Recovery tab.

   - View or change the user group security associations for this subclient from the Security tab.

   - Determine location from where archive logs will be backed up or deleted from the Log Destinations tab.

10. Click **OK** to save the subclient configuration. For QR Agents, this procedure is now complete. For all other agents, continue on to the next step.

11. The Backup Schedule dialog box advises you to schedule data protection operations for your new subclient. It is recommended you elect to set a schedule now. You can also associate this subclient with an All Agent Types schedule policy (which is automatically created by the system, or can be a user defined Data Protection schedule policy). If you have already associated a schedule policy at a previous level (Backup Set/Instance, Agent, Client, or Client Computer Group) the schedules defined in the Schedule Policy will be automatically applied to the new subclient. See Schedule Policy for more information.

    - If you want to associate this subclient with an All Agent Types schedule policy, click **Associate with Generic Schedule Policy**, and then select that schedule policy from the drop-down list box. Click **OK**.

    - If you want to associate this subclient with a specific schedule policy, click **Associate to schedule policy**, and then select the schedule policy from the drop-down list box. Click **OK**.

    - If you have selected to define a schedule for this subclient:

        - Click **Schedule**.

        - From the Backup/Archive Options dialog box, select the type of data protection operation that you want to schedule.

        - If you want to set Advanced Backup/Archive Options, click **Advanced**.

        - After selecting the data protection type and any advanced options, click **OK**. The **Schedule Details** dialog box appears.

- From the Schedule Details tab, select the scheduling options that you want to apply, then click **OK**.

○ If you don't want to create a data protection schedule at this time, click **Do Not Schedule,** and then click **OK**.

This task is now complete.

DELETE A DATA PROTECTION FILTER FROM A SUBCLIENT

Before You Begin

● Review Filters.

● Do not change the data protection or discovery filter of a subclient that has a data protection operation in progress.

● File Archiver for Windows/Unix Agents: We recommend that you don't delete the following entries from the exclusion filter, as it could cause your file system to be inoperable. For Windows, these include: *.dll, *.bat, *.exe, *.cur, *.ico, *.lnk. For Unix, these include *.a, *.ksh, *.csh, *.sh, *.lib, *.so.

Required Capability: Capabilities and Permitted Actions

To delete a data protection or discovery filter entry from a subclient:

1. From the CommCell Browser, right-click the subclient whose data protection or discovery filter you want to delete, and then click **Properties** from the shortcut menu.

2. Click the Filters tab of the Subclient Properties dialog box.

3. To delete an entry from the Exclusions list, click the entry in the upper pane then click the upper **Delete** button. (Repeat this step for each entry that you want to delete.)

4. To delete an entry from the Exceptions list (if applicable for your agent), click the entry in the lower pane then click the lower **Delete** button. (Repeat this step for each entry that you want to delete.)

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

NOTES

● Whenever you delete an entry from the exclusion filter, check if the exceptions list (i.e., lower pane) contains any entries that are children of the deleted data (if applicable for your agent). If so, you should delete them as described in Step 4 since they no longer need to be listed. The system automatically deletes any exceptions that are children of a deleted exclusion unless you used wildcard expressions in the exclusion path.

● When you change a data protection or discovery filter, the change is effective the next time the subclient is backed up/archived.

● Data will not be backed up in a differential backup for a subclient after a filter was removed.

● Since Incremental backups only back up data that has been modified since the last backup, previously filtered files whose filters are now removed, will not be backed up unless they have been modified since that last backup. To back up previously filtered files that have not been modified but whose filters have been removed since the last backup, you need to run a Full backup.

● Performing a full backup after changing filters or exceptions is recommended.

DELETE A USER-DEFINED SUBCLIENT

Related Topics:

● Command Line Interface - qdelete subclient

● Subclients

Required Capability: See Capabilities and Permitted Actions

To delete a user-defined subclient:

1. From the CommCell Browser, right-click the user-defined subclient that you want to delete, and then click **Delete** from the shortcut menu.

2. 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. If you click **Yes**:

   ○ the subclient, and any data that may have been protected/archived by the subclient are logically deleted, and you can no longer access the corresponding data for recovery/retrieve purposes. However, the data remains valid for the length of time specified by the associated retention period. Some agents allow you to browse data from a deleted subclient provided that the Browse Data Before date and time precedes the time that the user-defined subclient was deleted.

   ○ for agents that support a default subclient, once the user-defined subclient is deleted its contents are automatically reallocated to the default subclient the next time a data protection/archive/discovery operation is run on the default subclient to ensure data protection coverage.

   ○ the system deletes the selected subclient node and removes it from the CommCell Browser.

   ○ the system deletes any data protection/archive and recovery/retrieve job schedules that are associated with the subclient.

ENABLE OR DISABLE OPERATIONS

Required Capability: See Capabilities and Permitted Actions

Level	Capability
CommCell	Administrative Management with CommCell level association
Client Computer Group	Administrative Management with Client Computer Group level association
Client	Agent Management with Client level association
Agent	Agent Management with Agent level association
Subclient	Agent Management with Subclient level association

► To enable or disable activity control at the CommCell, client computer group, client, agent, or subclient levels:

1. From the CommCell Browser, right-click the CommServe, client computer group, client computer, agent, or subclient, and then click **Properties** from the short-cut menu.

2. From the Activity Control tab of the associated Properties dialog box, select or clear option(s), as desired.

3. Click **OK**.

> Disabled data management and/or data recovery operations are displayed with client and/or agent icon changes in the CommCell Browser. For a comprehensive list of all icons in the CommCell Console, see CommCell Console Icons.

ENABLE OR DISABLE SOFTWARE COMPRESSION FOR A SUBCLIENT

Before you Begin

● Do not enable/disable software compression for a subclient that is being backed up/archived.

Required Capability: Capabilities and Permitted Actions

► To enable software compression for a subclient:

1. From the CommCell Browser, right-click the subclient for which you wish to enable software compression and then click **Properties**.

2. Click the **Storage Device** tab and from the Data Storage Policy tab, select the storage policy from the **Storage Policy** list.

   If applicable for the selected agent, click the Log Storage Policy tab and select a storage policy from the **Transaction Log Storage Policy** list.

3. Then click the Storage Device (Data Transfer Option) tab and choose the appropriate compression option for this subclient.

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

This task is now complete.

REMOVE A PROCESS FROM PRE/POST PROCESSING OF DATA PROTECTION/ARCHIVE OPERATIONS

Before You Begin

● We recommend not removing a pre/post process for a subclient that is currently running a data protection or archive operation.

● Review the Overview and Agent-Specific Guidelines for your agent before removing pre/post processes for data protection/archive operations.

Required Capability: Capabilities and Permitted Actions

► To remove a process from Pre/Post processing of data protection/archive operations:

1. From the CommCell Browser, right-click the subclient for which you want to remove a pre/post process, and then click **Properties** from the shortcut menu.

2. Click the Pre/Post Process tab of the Subclient Properties dialog box.

3. Click the text inside the space that corresponds to one of the following phases for which you want a pre/post process removed, then press the **Delete** key:

   ○ PreScan
   ○ PreArchive
   ○ PreCopy
   ○ PreSnap
   ○ PostBackup
   ○ PostScan
   ○ PostArchive

- PostCopy
- PostSnap

4. Repeat Step 3 for any additional processes that you want to remove.

5. Click **OK**.

RENAME A SUBCLIENT

Before You Begin

- You can rename a subclient at any time. However, we recommend that you don't rename a subclient while a data protection or archive operation is running on that subclient.

- In cases where a subclient is renamed using the same name as a deleted subclient, the system will append a Unix time stamp to the deleted subclient's name in data protection job history reports and views to distinguish the two subclients. For example, *subclientname*_1104257351.

Required Capability: See Capabilities and Permitted Actions

To rename a subclient:

1. From the CommCell Browser, right-click the subclient that you want to rename, and then click **Properties** from the shortcut menu.

2. From the Subclient Properties (General) tab, or the QR Agent Subclient Properties (General) tab, type the new name in the **Subclient Name** field, and then click **OK**.

The CommCell Browser updates the subclient with its new name. The new name will also be reflected in any associated schedules and reports.

SET THE NETWORK BANDWIDTH AND NETWORK AGENTS FOR A DATA PROTECTION OPERATION

Before you Begin

- Do not modify the network bandwidth and network agents for a subclient or instance that is being backed up.

Required Capability: Capabilities and Permitted Actions

To Set the Network Bandwidth and Network Agents for a Data Protection Operation:

1. From the CommCell Browser, right-click a subclient and then click **Properties.**

   For the DB2, DB2 DPF, Informix, Oracle, Oracle RAC, SAP, or Sybase *i*DataAgent, right-click an instance and then click **Properties.**

2. Click the **Storage Device** Data Transfer Option tab.

   For the QR Agent:

   - To control network bandwidth settings, use the Throttle Network Bandwidth section in the General tab of the Subclient Properties dialog box.
   - To control the number of network agents, you must create a nQRNetworkAgents registry key.

3. Enter a number of **Network Agents** that must be used to perform data protection operations on the subclient/instance.

4. Click the **Throttle Network Bandwidth (MB/HR)** option and then enter the throughput as needed. Note that throttling is done on a per Network Agent basis.

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

This task is now complete.

VIEW DATA PATHS ASSOCIATED WITH A SUBCLIENT

Required Capability: See Capabilities and Permitted Actions

To view data paths:

1. From the CommCell Browser, right-click the subclient whose data paths you want to view, then click **Properties** from the shortcut menu.

2. Click the Storage Device tab of the Subclient Properties dialog box.

3. From the **Data [or Logs] Storage Policy** tab, click **Show Data Paths** to view the data paths used by the subclient to access the storage media for data protection operations. Click **Close** to exit the Data Paths dialog box.

4. Click **OK** to exit the Subclient Properties Storage Device tab.

VIEW SUBCLIENT CONTENT

Required Capability: See Capabilities and Permitted Actions

To view content of a subclient:

1. From the CommCell Browser, right-click the subclient whose content you want to view, then click **Properties**.

2. From the Subclient Properties dialog box, click the **Content** tab (or **Databases** tab for Lotus Notes) to view the contents of the subclient.

3. Click **OK** to close the dialog box.

DISABLE GLOBAL FILTERS ON A SUBCLIENT

Before You Begin

● Review Global Filters.

● Do not disable the Global Filter for a subclient that has a data protection operation in progress.

● Performing a full backup after disabling the Global Filter on a subclient is recommended.

● When you disable the Global Filter on a subclient, the change is effective the next time a data protection operation is run on the subclient.

Required Capability: Capabilities and Permitted Actions

To disable the Global Filter on a subclient:

1. From the CommCell Browser, right-click the subclient whose Global Filter you want to disable, and then click **Properties** from the shortcut menu.

2. Click the Filters tab of the Subclient Properties dialog box.

3. To disable Global Filters on this subclient, select one of the following values from the **Include Global Filters** list:
   ○ `OFF` - select this option to always disable Global Filters for this subclient.
   ○ `Use Cell Level Policy` - select this option to disable Global Filters for this subclient only when the **Use Global Filters on All Subclients** option is disabled on the **Control Panel (Global Filters)** dialog.

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

ADD/EDIT A DATA PROTECTION FILTER FOR A SUBCLIENT

Before You Begin

● Review Filters.

● Do not change the data protection or discovery filter of a subclient that has a data protection operation in progress.

● The system does not allow you to add entries that are not content of a particular subclient to that subclient's filter.

● For BlueArc and EMC Celerra (running at least DART OS 5.6.x) subclients, the filter string with or without wildcards must match the name or path of the file or directory being filtered.

● For NetApp subclients only name type filters (with wildcards) are supported:
   ○ You cannot enter paths as a filter (e.g. `/vol/vol0/data1`). Since NetApp does not support the use of paths in filters, if there are multiple files with the same name, even though they may be in different directories, all of them will be excluded from backups.
   ○ Name of the file or directory must exactly match the filter string.
   ○ You can specify a maximum of 32 strings in the exclude list.

Select the desired procedure:

● To add a data protection or discovery filter for a subclient

● To edit a data protection filter for a subclient

Required Capability: Capabilities and Permitted Actions

To add a data protection or discovery filter entry for a subclient:

1. From the CommCell Browser, right-click the subclient whose data protection or discovery filter you want to add, and then click **Properties** from the shortcut menu.

2. Click the Filters tab of the Subclient Properties dialog box.

3. For Exchange Mailbox, Exchange Mailbox/Public Folder Archiver Agents and Exchange Compliance Archiver, to specify a mailbox or folder that you want to exclude from data protection operations:
   ○ Click the upper **Add** button.

○ From the Browse window, expand the mailbox tree of the client computer.

○ Click the mailbox or folder that you want to exclude from the backup/archive operations on the selected subclient, and then click **Add**. (Repeat this step for each additional entry.)

○ From the Browse window, click **OK**.

The mailboxes or folders that you selected appear as entries in the upper pane. Repeat this step if you want to add more mailboxes and/or folders to the filter.

4. For NAS NDMP *i*DataAgents, click the **Add** button and, in the input window, type the name of the file, directory, (or path for BlueArc) that you want to exclude from the backups and click **OK**. The name displays as an entry in the **Exclude these files/folders/patterns** pane. Repeat this step if you want to add more files, directories, or paths to the filter.

5. For SharePoint Server *i*DataAgents, to specify a URL/file/folder/pattern that you want to exclude from data protection operations or to specify an exception filter for database backup sets, do one of the following:

○ Click the **Add** button next to **Exclude these files/folder/patterns**: input window and type the URLs of site collections that you want to exclude from the backups and click **OK**. The site collection displays as an entry in the **Exclude these files/folders/patterns** pane. Wildcards are supported. See Wildcards for more information. Repeat this step if you want to add more URLs, files, directories, or paths to the filter.

○ Click the **Add** button next to **Except for these files/folders**: input window and type the URLs/folders of site collections that you want to be exceptions for the exclusion filter and click **OK**. These exceptions will be included in the data protection operations. Wildcards are not supported for exception filters.

6. For Exchange Public Folder *i*DataAgents and SharePoint Server *i*DataAgent, to specify a workspace/folder that you want to exclude from the backups, click the upper **Browse** button and expand the *i*DataAgent of the client computer. Click the workspace/folder that you want to exclude from the backups and then click **Add**. Repeat this step for each additional entry.

7. For Windows/Unix/Macintosh File System *i*DataAgents, File Archiver for Windows/Unix Agents, and ProxyHost *i*DataAgent, to specify a file/folder/directory that you want to exclude from data protection operations, do one of the following:

○ Click the upper **Add** button and, in the **Enter Path** window, type the complete path (including drive letter) of the file/folder/directory that you want to exclude from the backups/archive operations. Repeat this step if you want to add more files/folders/directories to the filter.

○ Click the upper **Browse** button and expand the file system of the client computer. Click the file/folder/directory that you want to exclude from backups/archive operations and then click **Add**. Repeat this step for each additional entry.

8. For NetWare File System/NDS *i*DataAgents, to specify data that you want excluded from the backups, do one of the following:

○ To manually enter the path:

■ Click the **Add** button.

■ In the Input window, type the complete path (e.g., VOL1:\demo\disk2) of the data that you want to exclude.

■ Click **OK**. (The path that you typed displays as an entry in the upper pane.) Repeat this step if you want to exclude more data.

○ To browse and select a path:

■ Click the **Browse** button.

■ From the Backup Data window, expand the file system or NDS tree of the NetWare server.

■ Select the data that you want to exclude, and then click **Add**. Repeat this step for each additional entry.

■ From the Backup Data window, click **OK.** The data that you selected displays as entries in the upper pane.

9. For Lotus Notes Database and Lotus Notes Document *i*DataAgents, to specify a file or folder that you want to exclude from discovery, do one of the following:

○ Select the **Pattern/path to be excluded** field. Then type in a file or folder that you want to exclude. The format of the entry should start with a slash (\). The path entered is always relative to the data path of the partition. Then click **Add**. Repeat this step for each additional entry.

○ Click the upper **Browse** button and expand the file system of the client computer. Click the file or folder that you want to exclude from the backups and then click **Add**. Repeat this step for each additional entry.

10. For Exchange Mailbox, Exchange Mailbox/Public Folder Archiver Agents and Exchange Compliance Archiver, to specify a wildcard pattern of the folders that you want to exclude across all mailboxes within the subclient:

○ Click the lower **Add** button.

○ In the Input window, type the wildcard pattern of the folders that you want to exclude from backup/archive operations on the selected subclient.

○ Click **OK**. The path that you typed appears as an entry in the lower pane. Repeat this step if you want to add more entries to the filter.

11. For Exchange Public Folder *i*DataAgents and SharePoint Server *i*DataAgent, to specify an exception to an excluded workspace/folder (i.e., a folder/document that you want included in the backups, but whose parent directory has been excluded), click the lower **Browse** button and expand the *i*DataAgent of the client computer. Click the workspace/folder that you want to include in the backups and then click **Add**. Repeat this step for each additional entry.

12. For Windows/Unix/Macintosh File System *i*DataAgents, File Archiver for Windows/Unix Agents, and ProxyHost *i*DataAgent, to specify an exception to an excluded folder/directory (i.e., a file or folder/directory that you want included in the data protection operations, but whose parent folder/directory has been excluded), do one of the following:

- ○ Click the lower **Add** button and, in the **Enter Path** window, type the complete path (including drive letter) of the file/folder/directory that you want to include in the backups/archive operations. Repeat this step if you want to add more exceptions to the filter.

- ○ Click the lower **Browse** button and expand the file system of the client computer. Click the file/folder/directory that you want to include in the backups/archive operations and then click **Add**. Repeat this step for each additional entry.

13. For NetWare File System/NDS *i*DataAgents, to specify an exception to an excluded directory or NDS container (i.e., data that you want included in the backups, but whose parent directory or NDS container has been excluded), do one of the following:

    - ○ To manually enter the path:
        - Click the **Add** button.
        - In the Input window, type the complete path (e.g., VOL1:\demo\disk2\readme) of the data that you want to include.
        - Click **OK**.
    - ○ To browse and select a path:
        - Click the **Browse** button.
        - From the Backup Data window, expand the file system or NDS tree of the NetWare server.
        - Click the file or folder that you want to include in the backups and then click **Add**. Repeat this step for each additional entry.
        - Click **OK.** The selected data displays as entries in the lower pane.

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

Required Capability: Capabilities and Permitted Actions

▶ To edit a data protection filter entry for a subclient:

1. From the CommCell Browser, right-click the subclient whose data protection filter you want to edit, and then click **Properties** from the shortcut menu.

2. Click the Filters tab of the Subclient Properties dialog box.

3. Click the filter entry that you want to edit, and then click the **Edit** button associated with that pane.

4. Type the changes into the **Enter Path** dialog box, then click **OK**.

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

NOTES

- When you change a data protection or discovery filter, the change is effective the next time a data protection operation is run on the applicable subclient.

- Performing a full backup after changing filters or exceptions is recommended.

Back To Top

Archive History

Topics | How To | Related Topics

Overview

Items That Failed

Content Indexing Failures

Items that were Successfully Content Indexed

Pruning Backup History Information

Messages That Were Archived

OVERVIEW

The **Archive History Filter** dialog box allows you to view detailed, historical information about archive operations.

Once you have chosen your filter options, they are displayed in the **Archive Job History** window.

For information on Job Details displayed in the Job History, see Viewing Job Information.

From this window you can view more detailed information such as:

- The items that failed during the archive job.
- Files that were not indexed during an archive job that performed content indexing.
- Details of the archive job.
- Associated media.
- Events of the archive job.
- Messages that were archived.
- Log files of the archive job.

ITEMS THAT FAILED

The items that failed for a migration or archive operation include individual files or messages that may fail even though a particular archive operation completed successfully. You can determine the degree of success for these jobs by using this window.

Filters can be used in conjunction with the "Items That Failed" list on the data protection Job History Report to eliminate backup or archive failures by excluding items which consistently fail that are not integral to the operation of the system or applications. Some items fail because they are locked by the operating system or application and cannot be opened at the time of the data protection operation. This often occurs with certain system-related files and database application files.

CONTENT INDEXING FAILURES

Content Indexing failures allows you to look at the messages, files and documents that could not be indexed during a content Indexing operation. Content Indexing looks at each file (of the supported data types) and indexes its contents allowing advanced searches of backed up/archived data.

Files that were not indexed, (perhaps because the file's content could not be read) are added to the Content Indexing Failures list, and are viewable from the View Content Index (Failed Items) option in the Job History window. For step-by-step instruction, see View the Items that Failed to Content Index.

ITEMS THAT WERE SUCCESSFULLY CONTENT INDEXED

You can view the list of items that were successfully content indexed during a Content Indexing operation for a particular job. for step-by-step instructions, see View the Items that Were Successfully Content Indexed.

PRUNING BACKUP HISTORY INFORMATION

You can prune migration history information based on the number of days established in the **Days to keep the archive job histories** option from the **Media Management Configuration (Service Configuration)** dialog box available in the **Control Panel**.

MESSAGES THAT WERE ARCHIVED

You can view the messages that were archived during the archive operation by selecting the **View Archived Messages** option from an archive history window.

Back to Top

Archive Job History - How To

Topics | How To | Related Topics

View Archive Job History

View Job History Details

View the Events of a Job History

View the Media of a Job History

View the Items That Failed For a Data Protection Operation

View the Items that Were Not Indexed During Content Indexing

View the Items that Were Successfully Content Indexed

View Archived Messages

View the Log Files of a Job History

VIEW ARCHIVE JOB HISTORY

To view the job history of archive operations:

1. From the CommCell Browser, right-click the agent whose archive history you want to view, click **View**, then click **View Job History** -> **Archive**, or select **View Retrieve History**.

2. From the Archive Job History Filter, select the desired options, then click **OK**.

3. The system displays the Archive Job History window using the options you selected.

4. Click **OK**.

VIEW JOB HISTORY DETAILS

Required Capability: See Capabilities and Permitted Actions

To view the details of a job history:

1. From the CommCell Browser, right-click the entity (e.g., subclient, client computer, etc.) whose job history you want to view, click **View**, and then click job history.

2. From the Job History Filter dialog box, select the filter options that you want to apply and click **OK**.

3. From the Data Management Job History window, right-click the job whose job details you want to view, and then click **View Job Details**.

4. The Job Details dialog box appears, displaying detailed job history in General, Details, Phase Details and Attempts tabs for the selected job.

5. Click **OK**.

> If viewing the details of a job with a pending or failed status, the **Reason for Job Delay** field will contain an Error Code, which, if clicked, will launch the customer support website displaying troubleshooting article(s) related to the specific issue.

VIEW THE EVENTS OF A JOB HISTORY

Required Capability: See Capabilities and Permitted Actions

To view the events associated with a job:

1. From the CommCell Browser, right-click the entity (e.g., subclient, client computer, etc.) whose job history you want to view, click **View**, and then click

Job History.

2. From the Job History Filter dialog box, select the filter options that you want to apply and click **OK**.

3. From the Data Management Job History window, right-click the job whose job details you want to view, and then click **View Events**.

4. The All Found Events window gets displayed. If no events where found for the back up, a message is displayed to that effect.

5. Click **Close**.

VIEW THE MEDIA OR MOUNT PATHS OF A JOB HISTORY

To view media or mount paths associated with a job history:

1. From the CommCell Browser, right-click the entity (e.g., subclient, client computer, etc.) whose job history you want to view, click **View**, and then select the appropriate history.

2. From the Job History window select the filter options, if any, that you want to apply, and then click **OK**.

3. From the job history widow, right-click the backup whose media or mount paths you want to view, and then click **View Media**.

4. The Media Used By Job ID window displays a list of media or mount paths used by the operation.

5. Click **OK**.

VIEW THE ITEMS THAT FAILED FOR A DATA PROTECTION OPERATION

A listing of files and folders that failed is not available for the Quick Recovery Agent, nor the Image Level and Image Level ProxyHost *i*DataAgents. These agents do not perform a file level backup/copy.

To view the list of items that failed for a data protection operation:

1. From the CommCell Browser, right-click the entity whose history of data protection operations you want to view, click **View**, and then click to view a job history.

2. From the Job History Filter dialog box, select the filter options, if any, that you want to apply, and then click **OK**.

3. From the Job History window, right-click the operation whose list of failed items you want to view, and then select **View Failed Items**. The **Unsuccessful Backup Files** window (for DataArchiver Agents, **Items On Which Archive Failed**) displays those items that failed. If no items failed, a message to that effect is displayed.

4. Click **Close**.

VIEW THE ITEMS THAT FAILED TO CONTENT INDEX

This option is available for operations that performed content indexing.

To view the list of items that failed to content index:

1. From the CommCell Browser, right-click the entity whose operations you want to view, click **View**, and then click the necessary options to view a job history.

2. From the Job History Filter dialog box, select the filter options, if any, that you want to apply, and then click **OK**.

3. From the Job History window, right-click the job for which you want to view the list of items failed to content index, select **View Content Index**, and click **Failed Items**.

4. Click **Close**.

5. Click **Close** from the **Job History** window.

VIEW THE ITEMS THAT WERE SUCCESSFULLY CONTENT INDEXED

This option is available for operations that performed content indexing.

To view the list items that were not indexed during content indexing:

1. From the CommCell Browser, right-click the entity whose operations you want to view, click **View**, and then click the necessary options to view a job history.

2. From the Job History Filter dialog box, select the filter options, if any, that you want to apply, and then click **OK**.

3. From the Job History window, right-click the job for which you want to view the successfully content indexed items, select **View Content Index**, and click **Successful Items**.

4. Click **Close**.

5. Click **Close** from the **Job History** window.

VIEW ARCHIVED MESSAGES

To view the messages that were archived during an archive operation:

1. From the CommCell Browser, right-click the agent whose archive history you want to view, click **View**, then select **View Archive History**.

2. From the Archive History Filter, select the desired options, then click **OK**.

3. The system displays the Archive Job History window using the options you selected.

4. Right-click the appropriate archive job, then click **View Archived Messages**. The **Archived Messages List** window displays the messages that were archived during the archive operation.

5. Click **File ->Exit**.

VIEW THE LOG FILES OF A JOB HISTORY

Required Capability: See Capabilities and Permitted Actions

To view the log files of a Job History:

1. From the CommCell Browser, right-click the entity whose job history you want to view, and then click to view a job history.

2. From the job history filter window select the filter options, if any, that you want to apply, and then click **OK**.

3. From the job history window, right-click the job whose log files you want to view, and then click **View Logs**.

4. The contents of the log file related to the selected job history are displayed in the **Log File for Job *n*** window.

Back to Top

Recovery/Retrieve History

Topics | How To | Related Topics

Overview

Items That Recovered

- Showing Recovered Objects for DataArchiver Persistent Recovery Jobs

Pruning Recovery History Information

Recovery/Retrieve History Considerations

OVERVIEW

The **Recovery/Retrieve History Filter** dialog box allows you to view detailed, historical information about recovery or retrieve operations for the DataArchiver agents.

For information on Job Details displayed in the Job History, see Viewing Job Information.

Once chosen, your filter options are then displayed in the Recovery/Retrieve Job History window. From this window you can view more detailed information such as the:

- Items that did/did not recover during the recovery or retrieve job.
- Details of the recovery or retrieve job.
- Events of the recovery or retrieve job.
- Log files of the recovery or retrieve job.

If you want to change the number of days that DataArchiver recovery job history is kept, go to the Control Panel's Media Management Configuration (Data Aging) dialog box and change the settings for the **Days to keep the archiver restore job histories** field.

ITEMS THAT RECOVERED

The list of files that were recovered or retrieved by a data recovery or retrieve operation include those files that were successfully written back to the client file system are appended with the word:

- RESTORED (with the File Archiver Agent)
- RESTORED NEW (with the Exchange Mailbox/Public Folder Archiver Agents and the Exchange Compliance Archiver Agent)

Occasionally, data may not have been recovered or retrieved due to errors. Such data is appended with the word Not Restored.

Under some circumstances, the system may not recover or retrieve certain files because they are older versions of the same files already present in the files system. Such files are appended with the word OLDER. However, this word differs if the following recovery options are selected for Exchange Mailbox/Public Folder Archiver Agents:

- If the option Overwrite is selected then the message will have be appended with EXISTED, OVERWROTE.
- If the option Skip is selected, then the message will be appended with EXISTED, SKIPPED.

SHOWING RECOVERED OBJECTS FOR DATAARCHIVER PERSISTENT RECOVERY JOBS

The Show Recovered Objects List option may be unavailable from the Recovery History window for DataArchiver stub recovery jobs associated with a common open pipeline (i.e., *persistent recovery* jobs). This includes stub recoveries from disk media for File Archiver for Windows/Unix/NetWare, and stub recoveries from both tape and disk media for File Archiver for Windows/Unix/NetWare instances (Local File System, Celerra, FPolicy, Network File Share). In order to view the list of recovered objects for these DataArchiver persistent recovery jobs, select the View Job Details option then access the Job Details (Details) tab.

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.

PRUNING RECOVERY HISTORY INFORMATION

You can prune recovery history information based on the number of days established in the **Days to keep the archiver restore job histories** option from the Media Management Configuration (Data Aging) dialog box available in the **Control Panel**.

RECOVERY/RETRIEVE HISTORY CONSIDERATIONS

- Keep in mind that stub recall job history cannot be viewed for File Archiver for Windows recall jobs initiated from the physical node of a cluster in cases where only the driver is loaded on that node. However, browse recovery jobs which are initiated from the virtual server can still be viewed in job history. To obtain statistics on stub recall jobs in this scenario, we recommend running the Stub Recall Summary Report.

- When viewing the Recovery History of Stub Recalls (via the **Stub Recall Jobs** tab), it will be displayed as originating from the **defaultArchiveSet** and the first **Partition** even if a user-defined Archive Set or other partition were used during the recall. Partitions are applicable to Domino Mailbox Archiver.

Back to Top

Recovery History - How To

Topics | How To | Related Topics

View Recovery/Retrieve Job History

View Job History Details

View the Events of a Job History

View the Items Recovered for a Data Recovery Operation

View the Log Files of a Job History

VIEWING RECOVERY/RETRIEVE JOB HISTORY

To view the job history of recovery/retrieve operations:

1. From the CommCell Browser, right-click the agent whose recovery/retrieve history you want to view, click **View**, then click **Job History** -> **Recovery**, or click **View Retrieve History**.

2. From the Recovery/Retrieve History Filter select the desired options, then click **OK**.

3. The system displays the Recovery/Retrieve Job History window using the options you selected.

4. Click **OK**.

VIEW JOB HISTORY DETAILS

Required Capability: See Capabilities and Permitted Actions

To view the details of a job history:

1. From the CommCell Browser, right-click the entity (e.g., subclient, client computer, etc.) whose job history you want to view, click **View**, and then click job history.

2. From the Job History Filter dialog box, select the filter options that you want to apply and click **OK**.

3. From the Data Management Job History window, right-click the job whose job details you want to view, and then click **View Job Details**.

4. The Job Details dialog box appears, displaying detailed job history in General, Details, Phase Details and Attempts tabs for the selected job.

5. Click **OK**.

> If viewing the details of a job with a pending or failed status, the **Reason for Job Delay** field will contain an Error Code, which, if clicked, will launch the customer support website displaying troubleshooting article(s) related to the specific issue.

VIEW THE EVENTS OF A JOB HISTORY

Required Capability: See Capabilities and Permitted Actions

To view the events associated with a job:

1. From the CommCell Browser, right-click the entity (e.g., subclient, client computer, etc.) whose job history you want to view, click **View**, and then click **Job History**.

2. From the Job History Filter dialog box, select the filter options that you want to apply and click **OK**.

3. From the Data Management Job History window, right-click the job whose job details you want to view, and then click **View Events**.

4. The All Found Events window gets displayed. If no events where found for the back up, a message is displayed to that effect.

5. Click **Close**.

VIEW THE ITEMS THAT RESTORED/RECOVERED FOR A DATA RECOVERY OPERATION

To view the list of files that were restored/recovered for a data recovery operation:

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

2. From the Job History Filter window, select the filter options, if any, that you want to apply, and then click **OK**.

3. From the Job History window, right-click the job whose list of restored files you want to view, and then select **View Restore Files List** (for DataArchiver Agents select **Show Recovered Objects List**). The **Restored Files** window (for DataArchiver Agents it is the **Recovered Objects** window) displays those items that were restored/recovered. If no items failed, a message is displayed to that effect.

4. Click **Close**.

VIEW THE LOG FILES OF A JOB HISTORY

Required Capability: See Capabilities and Permitted Actions

To view the log files of a Job History:

1. From the CommCell Browser, right-click the entity whose job history you want to view, and then click to view a job history.

2. From the job history filter window select the filter options, if any, that you want to apply, and then click **OK**.

3. From the job history window, right-click the job whose log files you want to view, and then click **View Logs**.

4. The contents of the log file related to the selected job history are displayed in the **Log File for Job *n*** window.

Back to Top