

# Features - File Archiver for NetWare Agent

---

## TABLE OF CONTENTS

### OVERVIEW

#### SYSTEM REQUIREMENTS - FILE ARCHIVER FOR NETWARE AGENT

#### INSTALLATION

- Install the NetWare Server Agents - Express Install
- Install the NetWare Server Agents - Clustered Environment - Virtual Server

#### MIGRATION ARCHIVING - FILE ARCHIVER FOR NETWARE AGENT

#### RECOVER DATA - FILE ARCHIVER FOR NETWARE AGENT

#### CONFIGURATION

- Agents
- Archive Sets
- Subclients

#### MANAGEMENT

- Archive History
  - Recovery History
-

# Overview - File Archiver for NetWare Agent

---

This feature/product/platform is deprecated in this release. See [Deprecated Features, Products, and Platforms](#) for more information.

Choose from the following topics:

- [Introduction](#)
  - [Supported Data Types](#)
  - [Tree Levels in the File Archiver for NetWare Agent](#)
  - [License Requirement](#)
  - [Installation](#)
  - [Configuration](#)
  - [Archive and Recovery](#)
  - [Disaster Recovery Considerations](#)
- 

## INTRODUCTION

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

---

## SUPPORTED DATA TYPES

The File Archiver for NetWare Agent provides data protection support for all data types, except for those listed below.

---

### NOT RECOMMENDED FOR ARCHIVING

The following file types/objects are not recommended for archiving. Although it is possible to archive them, doing so could cause applications or the operating system to not function properly.

- Files with extensions `*.nlm`, `*.bat`, `*.exe`, `*.cur`, `*.ico`, and `*.lnk` are automatically filtered out of subclient content by default in the Subclient Properties (Filters) tab, therefore the system will not archive them.
- Application files/folders and disk mount path folders on which backup data resides, must be manually filtered out of subclient content. See [Add/Edit a Data Protection Filter for a Subclient for step-by-step instructions](#).

---

### NOT SUPPORTED FOR ARCHIVING

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

- Install folder
- Job Results folder
- Log files folder
- NetWare system folder
- Mountpoints to volumes
- Files with attributes of hidden, system, read-only or `REMOTE_DATA_INHIBIT`
- Files smaller than 4 KB

---

### SUPPORTED PROTOCOLS

- NCP with Novell client 4.91 SP2
- Data recalls by MAC clients are supported using the AFP protocol. (NetWare 6.5 with Support Pack 6 required)

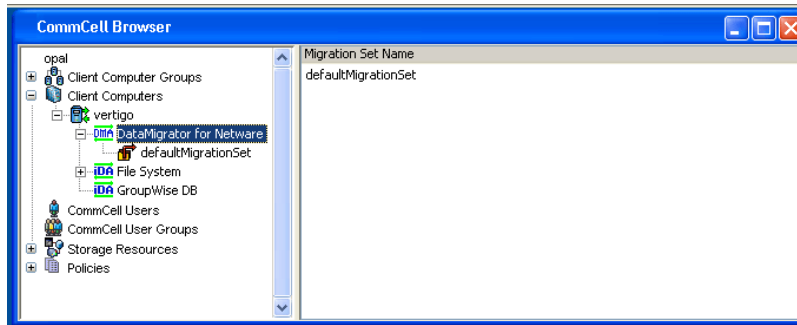
---

### SUPPORTED FILE SYSTEMS

- The File Archiver for NetWare Agent provides data protection support for native NSS volumes only.
-

## TREE LEVELS IN THE FILE ARCHIVER FOR NETWARE AGENT

When the File Archiver for NetWare Agent is installed, the following levels are automatically created in the CommCell Browser.



vertigo:Client

defaultArchiveSet: Archive Sets

File Archiver for NetWare: Agents



Before performing a Migration Archiving Operation using a File Archiver Agent, create a user-defined subclient. See Subclients - File Archiver for NetWare 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.

## INSTALLATION

Besides the CommServe and MediaAgent, there is one component to be installed for File Archiver for NetWare:

- File Archiver for NetWare Agent

For the procedures on installing this component, refer to Deployment - File Archiver for NetWare Agent.

## CONFIGURATION

The migration archiving operation is based on subclients, so the following configuration is per subclient basis. The following options are located in the subclient Properties (Rules) tab.

### ARCHIVING RULES

The configuration of the archiving rules is central to customizing migration archiving operations to meet the needs of your organization. For more information, see Overview.

- 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.

### INDEXING OPTION

To keep the index within a manageable size, a new index will be created every certain number of migration operations. This value can be entered in the "Set index cycle to every *n* archive jobs" field on the subclient properties Rules tab.

## ARCHIVE AND RECOVERY

---

## MIGRATION ARCHIVING

After configuration is completed, the recovery administrator can schedule migration archiving jobs, similar to scheduling backup jobs for *iDataAgents*. To ensure that only successfully archived files will be changed into stubs, the migration archiving operation is divided into two phases: archiving and stubbing. 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.

In the archiving phase, File Archiver for NetWare 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.

---

## RECOVERY

File Archiver for NetWare provides three ways to recover an archived file:

- Browse recovery from the CommCell Console (stand-alone application)
- Non-browse recovery from Windows Explorer on a Novell client workstation with a mapped network drive to a NetWare share
- Non-browse recovery from a NetWare system console

From the CommCell Console, the browse of File Archiver for NetWare data is forced to be a non-image browse to view all the archived files in this archiving cycle (since last creation of new index). The recovery administrator can browse and find the file to recover. To find files archived earlier than the last creation of new index, the administrator can provide a point-in-time in the *Browse Options* dialog box.

The second method of recovery, is recovering archived files from stubs in Windows Explorer by double-clicking the stubs.

The third method of recovery can be accomplished from the NetWare system console by performing any action that causes an open and read on the archived files, such as the `EDIT` command.

Refer to Recover Archived Data for more information on Recovery operations.

[Back to Top](#)

---

## DISASTER RECOVERY CONSIDERATIONS

The File Archiver for NetWare 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. File Archiver for NetWare relies upon the NetWare File System *iDataAgent* to perform a full system restore of client data. For more information, see *Restore Data - NetWare Server - Full System Restore*.

[Back to Top](#)

---

# System Requirements - File Archiver for NetWare Agent

This feature/product/platform is deprecated in this release. See [Deprecated Features, Products, and Platforms](#) for more information.

The following requirements are for the File Archiver for NetWare:

## APPLICATION

NetWare 6.5 up to Support Pack 8

NetWare 6.5 Branch Office with Support Pack 5 (Not supported along with the resync replication feature.)

## CLUSTER - SUPPORT

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

For information on supported cluster types, see [Clustering - Support](#).

## HARD DRIVE

1 GB of minimum disk space is required for installing the software.

256 MB of free disk space is required for job result directory.

256 MB of free disk space is required for log directory.

## MEMORY

32 MB RAM per stream/drive minimum required beyond the requirements of the operating system and running applications

## PROCESSOR

Intel Pentium or compatible minimum required

## PERIPHERALS

DVD-ROM drive

Network Interface Card

## MISCELLANEOUS

Novell NetWare TCP/IP Services configured on the computer.

Novell's Storage Management Service (SMDR.NLM) must be loaded.

The software must be installed on an NSS volume.

You must have some form of name resolution between your CommServe, NetWare Server, and MediaAgent to ensure proper operations. It is recommended that your NetWare server has DNS services configured.

The NetWare File System *iDataAgent* will be automatically installed during installation of the File Archiver for NetWare Agent, if the File System *iDataAgent* is not already installed.

## DISCLAIMER

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

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

# Install the NetWare Server Agents - Express Install

## TABLE OF CONTENTS

### Install Requirements

#### Before You Begin

#### Install Procedure

- Getting Started
- Select Components for Installation
- Firewall Configuration
- Configuration of Other Installation Options
- Schedule Automatic Update
- Configure Client Name
- Storage Policy Selection
- Configure Account Information
- Verify Summary of Install Options
- Setup Complete

#### Post-Install Considerations

## INSTALL REQUIREMENTS

The NetWare Agents are remotely installed from a Novell Client computer to the NetWare Server(s). This installation procedure describes the installation of all four NetWare Agents:

- NDS iDataAgent
- NetWare File System iDataAgent
- Novell GroupWise iDataAgent
- File Archiver for NetWare Agent

Verify that the NetWare server to which you are installing and the Novell client from which you are installing satisfies the minimum requirements specified in the following System Requirements:

- System Requirements - NetWare Server for NetWare File System and NDS iDataAgents
- System Requirements - Novell GroupWise iDataAgent
- System Requirements - File Archiver for NetWare Agent

In order to secure the File System data on all NetWare servers, you must install the File System iDataAgent to each NetWare server.

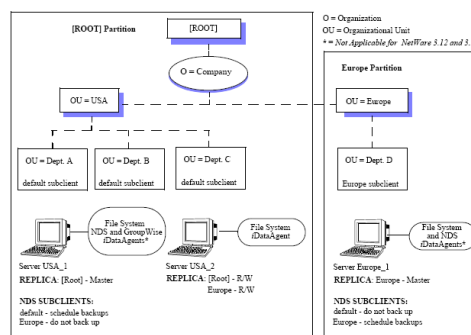
In order to secure GroupWise data, the GroupWise iDataAgent must be installed on each GroupWise server.

When you select the File Archiver for NetWare Agent for install, the NetWare File System iDataAgent is automatically selected for install.

It is not necessary to install the NDS iDataAgent to every NetWare server because the same NDS data can be backed up from any server in the same tree. You may want to split your NDS backup to match your partitions. See the figure below for an example NDS installation.

**Example:** This diagram illustrates a typical NDS installation. The tree, Company, consists of two partitions, hence two replica rings. Notice that while the File System iDataAgent is installed on all the servers, the NDS iDataAgent is installed on one server from each of the replica rings. The NDS iDataAgent is not installed on server USA\_2, as their NDS data will be secured through server USA\_1.

For maximum efficiency, it is recommended that you select one NetWare server in each replica ring, and install the NDS iDataAgent to this server.



## CUSTOM AND EXPRESS INSTALLATION MODES

The install program allows you to install multiple MediaAgents and Agents at the same time, using either the Express or Custom installation modes. If you are installing on only one computer the modes do not apply.

### CUSTOM INSTALLATION MODE

The custom mode is useful to customize each installation. Use the Custom mode when you wish to:

- Install MediaAgents and/or Agents attached to multiple CommServes

- Assign unique configurations for each of the MediaAgents and/or Agents

For step-by-step instruction on installing the NetWare Agent using the custom mode, see [Install the NetWare Server Agents - Custom Install](#).

### EXPRESS INSTALLATION MODE

The Express mode is useful to rapidly install multiple MediaAgents and/or Agents. Use the Express mode when all the MediaAgents and/or Agents that you wish to install can have the following options:

- The same CommServe
- The same path structure for the install directory
- The same path structure for the Index Cache directory (for MediaAgents)
- The same path structure for the Job Results directory

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.

---

### AGENT SPECIFIC

- If there is an agent installed on the Novell Client computer you will be using to run the installation, then configuring firewall settings will conflict with running services. To prevent this, stop all running base services on the Novell Client computer before you begin installation. Start them after the installation is complete. For more information, see [Services](#).
- If your network does not have the DNS lookup or some other name resolution facility, open the hosts file and enter the FQDN (Fully Qualified Domain Name) and IP address of the CommServe computer. The host's file is usually located in the SYS:\ETC directory.

### BEFORE YOU BEGIN

- From a Novell client, log on to the NetWare server you want to install as a user with Supervisor rights or use an account that has Read/Write/Modify/Erase/Create/File Scan rights to the SYS:SYSTEM directory.
- For the Novell GroupWise iDataAgent, either the GW TSA.NLM or the TSAFSGW.NLM should be loaded prior to install.

### INSTALL PROCEDURE

---

#### GETTING STARTED

1. Create the bIgnoreCommServeVersion registry key.

To create the registry key, see the following steps:

- Click **Start**, click **Run**, type **regedit**, and then click **OK**.
- Navigate to the following directory:

```
HKEY_LOCAL_MACHINE\SOFTWARE\
```

- Right click the SOFTWARE and click **New -> Key**.
- Name the key as GalaxyInstallerFlags.
- Right click the GalaxyInstallerFlags and select **New -> DWORD** value, name it as bIgnoreCommServeVersion
- Double-click the bIgnoreCommServeVersion key modify the **Value data** to **1**.

2. Place the software installation disc for the Windows platform into the Novell client's disc drive or a mapped disc drive on another computer or a network share.

If the installation menu does not appear:

- a. Click **Start** on the Windows task bar, and then click **Run**.
- b. Browse the installation disc drive, right-click **Setup.exe**, then click **Open**.

In the language screen, click the down arrow, select the desired language from the pull-down list, and then click **Next** to continue.

3. Select the option to install software on a NetWare server.

**NOTES**

- The options in this menu depend on the computer in which the software is being installed.
4. Read the Welcome screen.  
Click **Next** to continue, if no other applications are running.
  5. Select **Install** from the Install/Uninstall Selection screen.  
Click **Next** to continue.
  6. Read the license agreement, then select **I accept the terms in the license agreement**.  
Click **Next** to continue.

**SELECT COMPONENTS FOR INSTALLATION**

7. The install program automatically discovers the available NetWare servers.  
Select the NetWare server(s) to which you want to install the Agent(s). You can select multiple servers, provided you have supervisor rights on each one.

**NOTES**

- If the install program was unable to discover an existing server, its name can be added to the Available Servers list by manually entering the name, and clicking **Add Server**.
- To add and remove existing servers to and from the Selected Servers list, use the **Add** and **Remove** buttons.
  - If you are not logged on to the selected server(s), the Novell Login dialog box appears. To install software to the server(s), you must log on as a user with Supervisor rights or use an account that has Read/Write/Modify/Erase/Create/File Scan rights to the SYS:SYSTEM directory.
  - If your account on any available NetWare server does not have the appropriate rights, a dialog box warns you that you do not have the authority to install to that server. The server remains in the list of available servers. To install to that server, you must log off and log back on as a user with the appropriate rights.

Click **Next** to continue.

8. Select any or all of following the Agent(s) you want to install.

- iDataAgent for NetWare File System
- iDataAgent for Novell Directory Services (NDS)
- iDataAgent for NetWare GroupWise
- NetWare MediaAgent
- Agent for NetWare File System DataArchiver

**NOTES**

- This screen is repeated for each server selected for installation.
- If you are installing the NDS iDataAgent, it is recommended that you install it to one NetWare server on each partition in order to increase the efficiency of back up and restore procedures. See Install Requirements for more details.
- If you are installing the NetWare File System DataArchiver, then the NetWare File System iDataAgent is automatically selected for install.
- The GroupWise iDataAgent will only be selectable for installation on GroupWise servers.

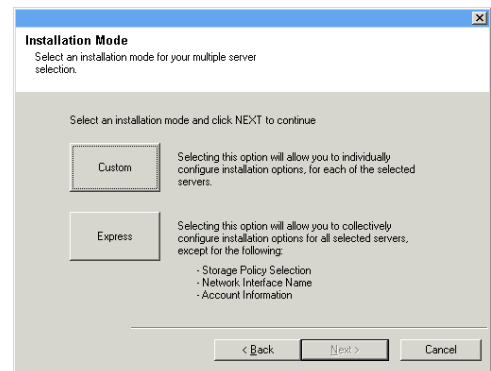
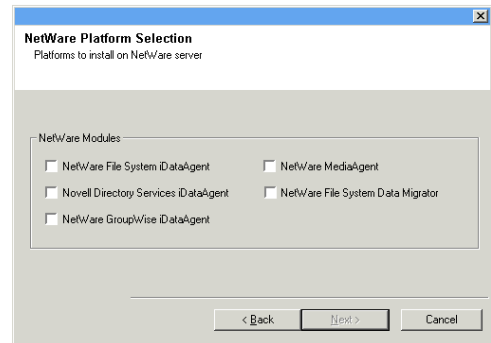
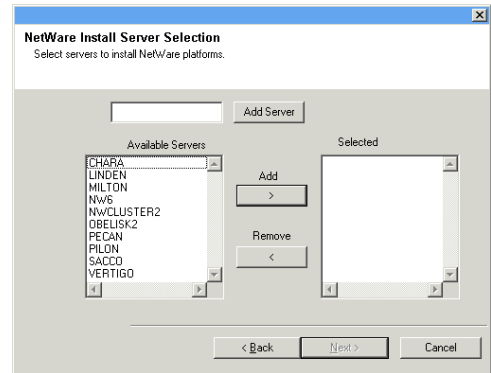
Click **Next** to continue.

9. Select **Express** to install the software and assign common installation options across all servers in one pass.

**NOTES**

- In Express mode, the install program leads you through an install in which you assign common installation options across all servers in one pass. Use this mode to expedite your install if you are configuring multiple servers to the same CommServe.
- In Custom mode, the install program leads you through an install in which you assign unique configurations for each of the selected NetWare servers in turn. While configuring options, each dialog box clearly indicates if you are working in Express mode or working on a specific server's configuration settings.
- This screen will not appear if you have only selected one server for installation.

Click **Next** to continue.



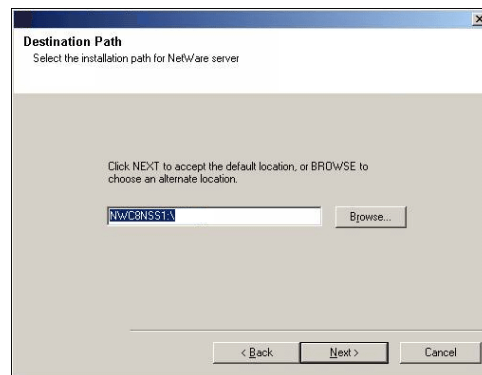


- Accept the default Destination Path or enter an alternate install path.

**NOTES**

- In an Express install the Browse button is disabled.
- Destination folders:
  - must follow DOS naming conventions
  - must not exceed a length of 8.3 characters
  - must not use the following characters when specifying the destination folder:  
/ : \* ? " < > |  
It is recommended you use alphanumeric characters only.

Click **Next** to continue.



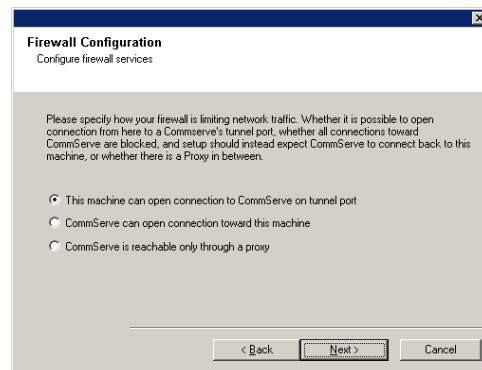
**FIREWALL CONFIGURATION**

- Select from the following:

- If this Client communicates with the CommServe Server and/or MediaAgent across a firewall, select **Yes, configure firewall services**, and then click **Next** to continue. Proceed to the next Step.
- If firewall configuration is not required, click **No, do not configure firewall services** and then click **Next** to continue. Proceed to the next section.

**NOTES**

- Operating systems, such as Windows 2008 and Windows Vista, may have more than one profile present. When you select **No** to configure firewall services, verify that firewall settings are not enabled in the profile(s).
- If the system detects firewall settings are present in the profile(s), you must select from the following:
  - Disable firewall for ALL profiles:** Employ caution when choosing this option; firewall settings will be disabled in all profiles. This requires a system reboot; installation automatically resumes after reboot.
  - No, Firewall is not enabled:** Select this option if your firewall settings allow communication with the CommServe computer. Click Back to configure firewall services.



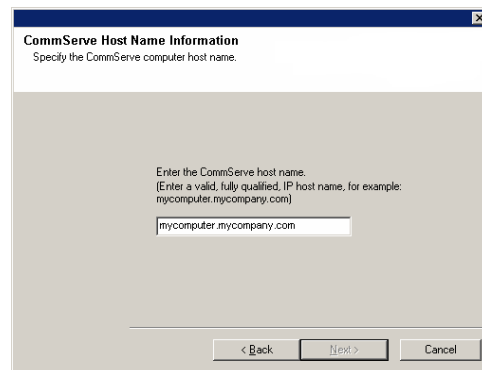
**CONFIGURATION OF OTHER INSTALLATION OPTIONS**

- Enter the fully qualified domain name of the CommServe computer. (TCP/IP network name. e.g., computer.company.com)

**NOTES**

- Do not use spaces when specifying a new name for the CommServe Host Name.
- If a component has already been installed, this screen will not be displayed; instead, the installer will use the same Server Name as previously specified.

Click **Next** to continue.

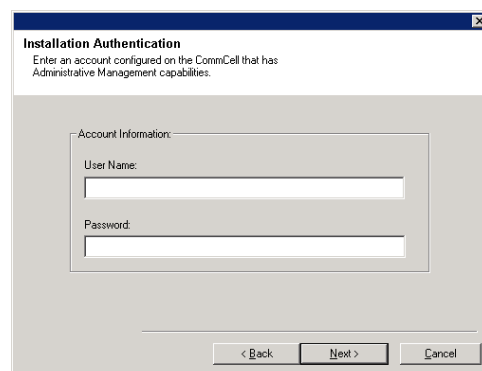


- Enter the **username** and **password** associated with an external domain user account or a CommCell user account to authorize the installation of this agent.

**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.

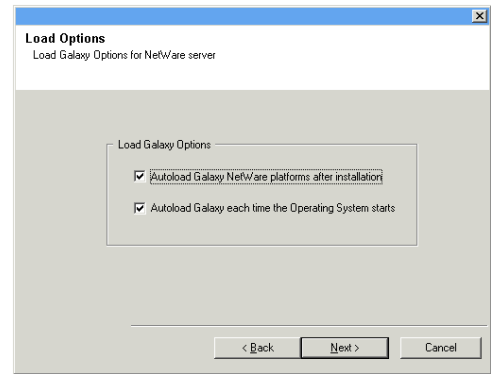


14. Select one of the Load Options:
- Automatically load the software onto the server after installation.
  - Automatically load the software each time you restart the server.

**NOTES**

- If you choose not to autoloading the agents after installation, you will need to manually load the Agents onto each server after completing the installation.

Click **Next** to continue.



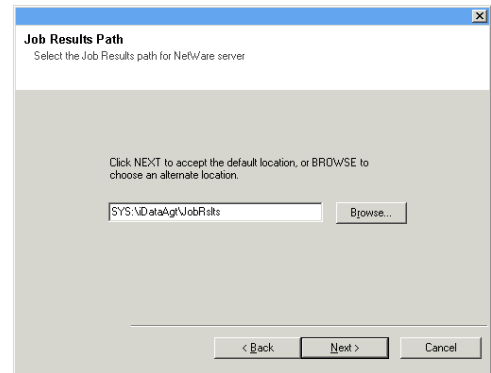
15. Specify the location of the client's job results directory.

**NOTES**

- The Agent uses the job results directory to store the client's backup and restore job results.
- In an Express install the Browse button is disabled.
- Job results folders:
  - must follow DOS naming conventions
  - must not exceed a length of 8.3 characters
  - must not use the following characters when specifying the destination folder: % \* ? < > |  
It is recommended you use alphanumeric characters only.

Click **Browse** to change directories.

Click **Next** to continue.



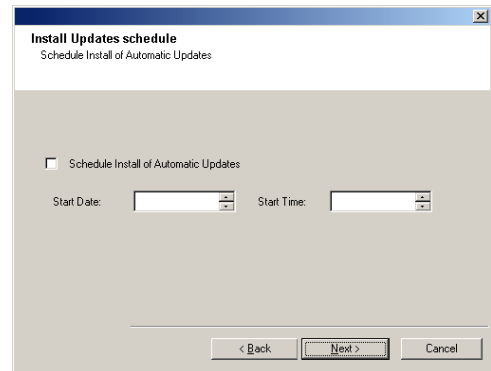
**SCHEDULE AUTOMATIC UPDATE**

16. 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.



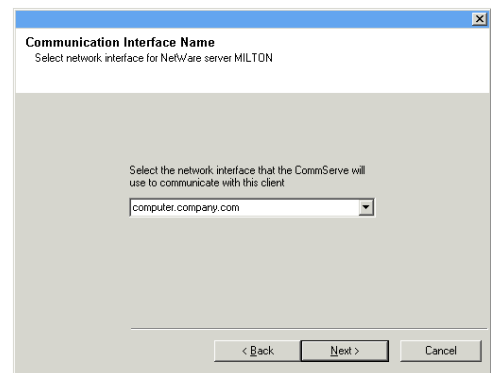
**CONFIGURE CLIENT NAME**

17. Enter either of the following:
- If resolvable, 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.

**NOTES**

- This dialog box will appear once for each server selected for installation. For example, if you are installing four servers, this dialog box will appear four times.
- The name of the NetWare server you are configuring is indicated in each screen. In an Express install, this dialog box will repeat for each server selected for installation.

Click **Next** to continue.



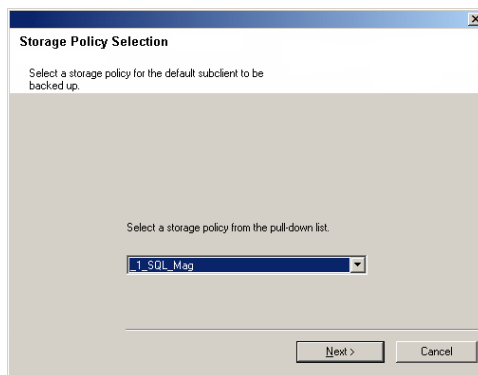
**STORAGE POLICY SELECTION**

- Configure storage policies for the NetWare File System if selected for installation. Select the storage policy through which you want to back up/archive the indicated component (subclient, instance, etc.)

**NOTES**

- A storage policy directs backup data to a media library. Each library has a default storage policy.
- When you install an Agent, the install program creates a default subclient for most Agents.
- If desired, you can change your storage policy selection at any time after you have installed the client software.
- If this screen appears more than once, it is because you have selected multiple agents for installation and are configuring storage policy association for each of the installed agents.

Click **Next** to continue.



**CONFIGURE ACCOUNT INFORMATION**

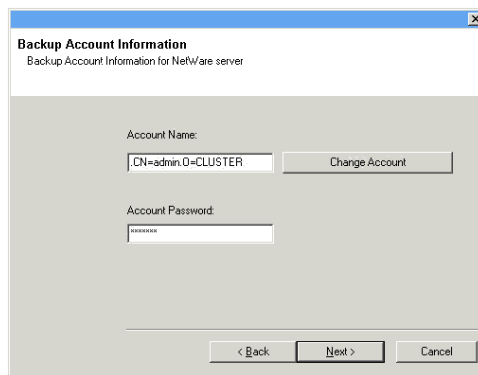
- Enter the Backup Account Information. By default, the install program uses the account of the user currently logged into the NetWare server.
  - To use the default user account, enter the password of that account.
  - To select a different user account, click **Change Account**. In the Select User dialog box, select from the tree of NetWare user accounts, and click **OK**.
  - To create a new user account, click **Change Account**. Then click **Create New User**. Enter the required account information, assign the desired rights to the new user, and click **Create**. The install program creates the account. In the Select User dialog box, select the new account from the tree, and click **OK**.

**NOTES**

- In order to effectively back up and restore data, you must select a user account with the appropriate rights.
  - For the File System *iDataAgent*, GroupWise *iDataAgent* and File Archiver for NetWare Agent, it is recommended that the user account have supervisor rights to the server.
  - For the NDS *iDataAgent*, you must select a NetWare user account with supervisor rights to the root of the entire NDS tree.
- Changing a network account requires about five minutes to be synchronized.

Click **Next** to continue.

See the NetWare Server *iDataAgents* section in **User Accounts and Passwords** for more information.



**VERIFY SUMMARY OF INSTALL OPTIONS**

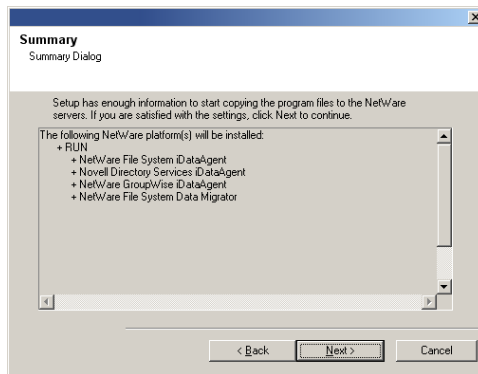
- Verify the summary of selected options.

**NOTES**

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

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

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



**SETUP COMPLETE**

- Setup displays the successfully installed components.

**NOTES**

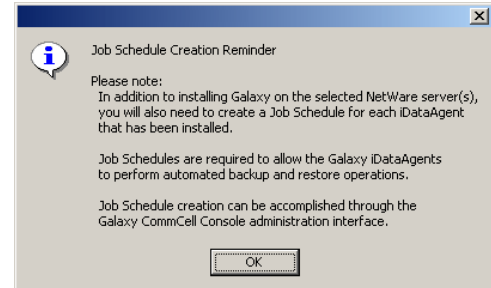
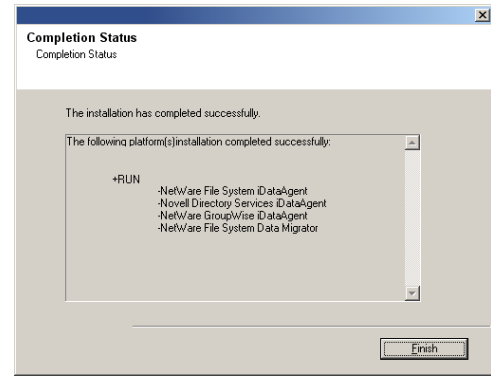
- The **Setup Complete** message displayed on your screen will reflect the components you installed, and may look different from the example shown.
- If you install an Agent with the CommCell Console open, you need to refresh the CommCell Console (F5) to see the new Agents.

Click **Finish** to continue.

22. Click **OK** to exit the install program.  
The installation is now complete.

#### 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.



## POST-INSTALL CONSIDERATIONS

### GENERAL

- Install post-release updates or Service Packs that may have been released after the release of the software. When you are installing a Service Pack, ensure that it is the same version as the one installed in the CommServe Server. Alternatively, you can enable Automatic Updates for quick and easy installation of updates in the CommCell component.
- After installing the Agent, you may want to configure the Agent before running a data protection operation. The following list includes some of the most common features that can be configured:
  - Configure your subclients - see Subclients for more information.
  - Schedule your data protection operations - see Scheduling for more information.
  - Configure Alerts - See Alerts and Monitoring for more information.
  - Schedule Reports - See Reports for more information.

The software provides many more features that you will find useful. See the Index for a complete list of supported features.

### AGENT SPECIFIC

- For the GroupWise iDataAgent, depending on your GroupWise system configuration, either the GWTS.NLM or the TSAFSGW.NLM should be loaded prior to install as well as prior to loading client services each time the server is rebooted.  
If either the GWTS.NLM or the TSAFSGW.NLM is not loaded, use the appropriate NetWare Command File (NCF) to load the NLM. The following example pertains to the GWTS.NLM, but also applies to the TSAFSGW.NLM:
  - Build the GWTS.NCF file to specify where the GroupWise directories are located on the system using the following arguments:
 

```
LOAD SYS:\SYSTEM\SMDR
LOAD SYS:\SYSTEM\GWTS /HOME-GROUPWISE:\GRPWISE\CVGWDOM\ /HOME-GROUPWISE:\GRPWISE\CVGWPO
```
- The following configuration tasks are required before performing an Archive Operation using this Archiver Agent:
  - Create a Subclient - see Subclients - File Archiver for NetWare for more information.
  - Archiving Rules are initially disabled by default. You must clear the **Disable All Rules** option in the Subclient Properties (Archiving Rules) or (Rules) tab and configure the archiving rules before conducting rules-based Archive Operations.

### DISASTER RECOVERY CONSIDERATIONS

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

# Install the NetWare Server Agents - Clustered Environment - Custom Install

## TABLE OF CONTENTS

### Install Requirements

#### Before You Begin

#### Install Procedure

- Getting Started
- Select Components for Installation
- Destination Path
- Configuration of Other Installation Options
- Schedule Automatic Update
- Configure Client Name
- Storage Policy Selection
- Configure Account Information
- Verify Summary of Install Options
- Setup Complete

#### Post-Install Considerations

## INSTALL REQUIREMENTS

The following NetWare Server Agents can be installed in the cluster group:

- NetWare File System *iDataAgent*
- File Archiver for NetWare Agent
- Novell GroupWise *iDataAgent*

The NetWare File System *iDataAgent*, File Archiver for NetWare Agent, and Novell GroupWise *iDataAgent* are remotely installed from a Novell Client computer to the NetWare Server(s). This installation procedure describes the installation for both of these NetWare Agents.

The NetWare File System *iDataAgent* must be installed on all of the Physical nodes in the cluster before installing any NetWare Agents/MediaAgents in the cluster group. Installs in the cluster group are always Custom installs. Furthermore, all physical and virtual servers within a cluster must be installed to the same CommServe.

See Install the NetWare Server *iDataAgents* - Express Install or Install the NetWare Server *iDataAgents* - Custom Install for instructions on installing the NetWare File System *iDataAgent* to the physical node.

Once the NetWare File System *iDataAgent* has been installed onto the physical node, the NetWare File System *iDataAgent*, File Archiver for NetWare Agent, and Novell GroupWise *iDataAgent* can be installed in the cluster group using the following procedure. When the virtual server install procedure is performed, an automated configuration of the `Galaxy.INI` file is performed on all available nodes at the same time.

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

Verify that the NetWare server to which you are installing and the Novell client from which you are installing satisfy the minimum requirements specified in the following System Requirements:

- System Requirements - NetWare Server *iDataAgents* for NetWare File System *iDataAgent*
- System Requirements - File Archiver for NetWare Agent
- System Requirements - Novell GroupWise *iDataAgent*

The following procedure describes the steps involved in installing the NetWare File System *iDataAgent* and the File Archiver for NetWare Agent. Note that if you have already installed the NetWare File System *iDataAgent*, the sequence of the install steps may vary for the File Archiver for NetWare Agent when installed separately.

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 there is an agent installed on the Novell Client computer you will be using to run the installation, then configuring firewall settings will conflict with running services. To prevent this, stop all running base services on the Novell Client computer before you begin installation. Start them after the installation is complete. For more information, see [Services](#).
- If your network does not have the DNS lookup or some other name resolution facility, open the hosts file and enter the FQDN (Fully Qualified Domain Name) and IP address of the CommServe computer. The host's file is usually located in the SYS:\ETC directory.

---

## CLUSTER

- Check the following on the cluster computer in which you wish to install the software:
  - Cluster software is installed and running.
  - Active and passive nodes are available.
  - Disk array devices configured with access to the shared array.
  - Public Network Interface Card is bound first, before the private Network Interface Card. (Does not apply to NetWare Cluster.)

## BEFORE YOU BEGIN

From a Novell client, log on to the NetWare server you want to install as a user with Supervisor rights or use an account that has Read/Write/Modify/Erase/Create/File Scan rights to the SYS:SYSTEM directory.

## INSTALL PROCEDURE

---

### GETTING STARTED

1. Create the bIgnoreCommServeVersion registry key.

To create the registry key, see the following steps:

- Click **Start**, click **Run**, type **regedit**, and then click **OK**.
- Navigate to the following directory:

```
HKEY_LOCAL_MACHINE\SOFTWARE\
```

- Right click the **SOFTWARE** and click **New -> Key**.
- Name the key as **GalaxyInstallerFlags**.
- Right click the **GalaxyInstallerFlags** and select **New -> DWORD** value, name it as **bIgnoreCommServeVersion**
- Double-click the **bIgnoreCommServeVersion** key modify the **Value data** to **1**.

2. Place the software installation disc for the Windows platform into the Novell client's disc drive or a mapped disc drive on another computer or a network share.

If the installation menu does not appear:

- a. Click **Start** on the Windows task bar, and then click **Run**.
- b. Browse the installation disc drive, right-click **Setup.exe**, then click **Open**.

In the language screen, click the down arrow, select the desired language from the pull-down list, and then click **Next** to continue.

3. Select the option to install software on a NetWare server.

#### NOTES

- The options in this menu depend on the computer in which the software is being installed.

4. Read the Welcome screen.

Click **Next** to continue, if no other applications are running.

5. Select **Install** from the Install/Uninstall Selection screen.

Click **Next** to continue.

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

Click **Next** to continue.

---

### SELECT COMPONENTS FOR INSTALLATION

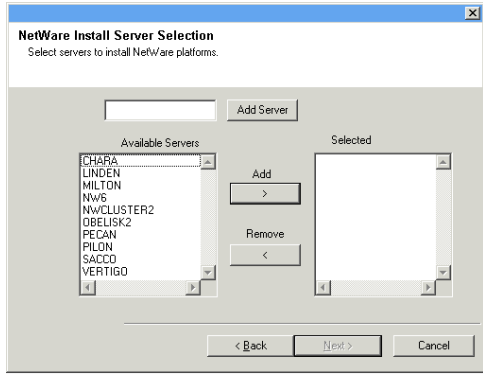
7. The install program automatically discovers the available NetWare servers.

Select the NetWare server(s) to which you want to install the Agent(s). You can select multiple servers, provided you have supervisor rights on each one.

#### NOTES

- If the install program was unable to discover an existing server, its name can be added to the Available Servers list by manually entering the name, and clicking **Add Server**.
- To add and remove existing servers to and from the Selected Servers list, use the **Add** and **Remove** buttons.
  - If you are not logged on to the selected server(s), the Novell Login dialog box appears. To install software to the server(s), you must log on as a user with Supervisor rights or use an account that has Read/Write/Modify/Erase/Create/File Scan rights to the SYS:SYSTEM directory.
  - If your account on any available NetWare server does not have the appropriate rights, a dialog box warns you that you do not have the authority to install to that server. The server remains in the list of available servers. To install to that server, you must log off and log back on as a user with the appropriate rights.

Click **Next** to continue.



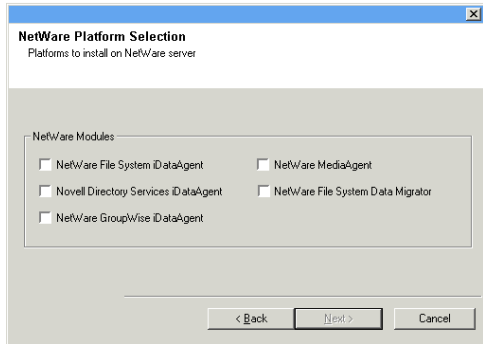
**8.** Select either or both of following the Agents you want to install.

- iDataAgent for NetWare File System
- Agent for NetWare File System DataArchiver
- NetWare GroupWise iDataAgent

**NOTES**

- This screen is repeated for each server selected for installation.
- If you are installing the NetWare File System DataArchiver, then the NetWare File System iDataAgent is automatically selected for install unless it has already been installed.
- The NDS iDataAgent is not supported for installation in the cluster group.

Click **Next** to continue.



**9.** If you select more than one server to be installed, a message will appear stating that since you have selected virtual servers you can only proceed in custom mode.

Click **OK** to continue.

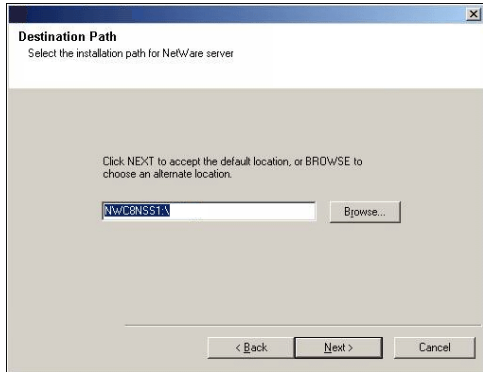
**DESTINATION PATH**

**10.** Accept the default Destination Path or enter an alternate install path.

**NOTES**

- In an Express install the Browse button is disabled.
- Destination folders:
  - must follow DOS naming conventions
  - must not exceed a length of 8.3 characters
  - must not use the following characters when specifying the destination folder: / : \* ? " < > |  
It is recommended you use alphanumeric characters only.

Click **Next** to continue.



**CONFIGURATION OF OTHER INSTALLATION OPTIONS**

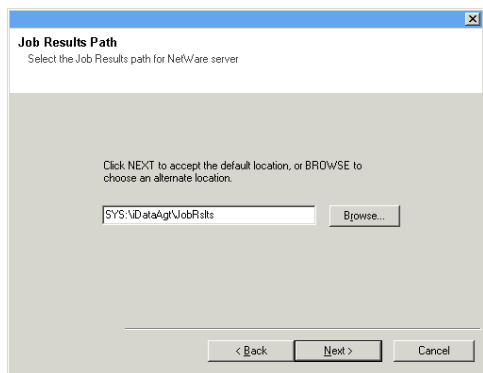
**11.** Specify the location of the client's job results directory.

**NOTES**

- The Agent uses the job results directory to store the client's backup and restore job results.
- In an Express install the Browse button is disabled.
- Job results folders:
  - must follow DOS naming conventions
  - must not exceed a length of 8.3 characters
  - must not use the following characters when specifying the destination folder: % \* ? < > |  
It is recommended you use alphanumeric characters only.

Click **Browse** to change directories.

Click **Next** to continue.



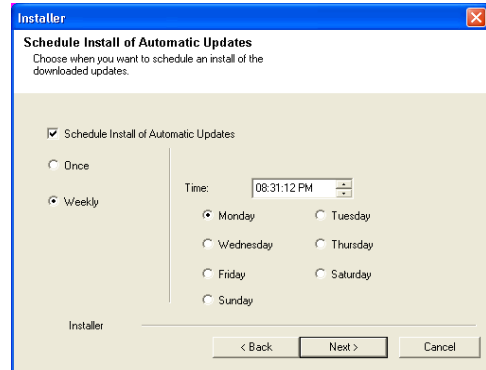
## SCHEDULE AUTOMATIC UPDATE

12. 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.



## CONFIGURE CLIENT NAME

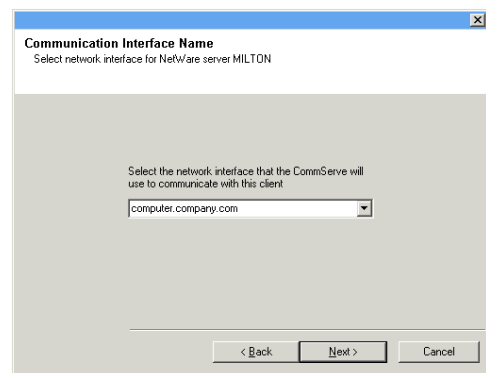
13. Enter either of the following:

- If resolvable, 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.

### NOTES

- This dialog box will appear once for each server selected for installation. For example, if you are installing four servers, this dialog box will appear four times.
- The name of the NetWare server you are configuring is indicated in each screen. In an Express install, this dialog box will repeat for each server selected for installation.

Click **Next** to continue.



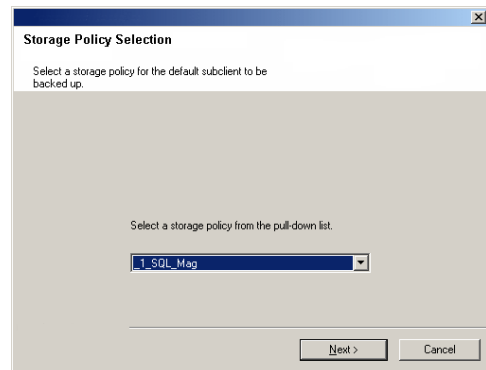
## STORAGE POLICY SELECTION

14. Select the storage policy through which you want to back up/archive the indicated component (subclient, instance, etc.)

### NOTES

- A storage policy directs backup data to a media library. Each library has a default storage policy.
- When you install an Agent, the install program creates a default subclient for most Agents.
- If desired, you can change your storage policy selection at any time after you have installed the client software.
- If this screen appears more than once, it is because you have selected multiple agents for installation and are configuring storage policy association for each of the installed agents.

Click **Next** to continue.



## CONFIGURE ACCOUNT INFORMATION

15. Enter the Backup Account Information. By default, the install program uses the account of the user currently logged into the NetWare server.

- To use the default user account, enter the password of that account.
- To select a different user account, click **Change Account**. In the Select User dialog box, select from the tree of NetWare user accounts, and click **OK**.
- To create a new user account, click **Change Account**. Then click **Create New User**. Enter the required account information, assign the desired rights to the new user, and click **Create**. The install program creates the account. In the Select User dialog box, select the new account from the tree, and click **OK**.

### NOTES

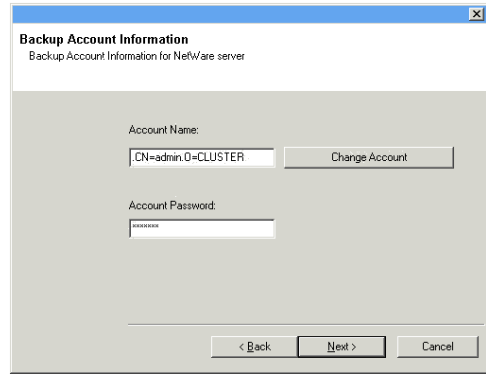
- In order to effectively back up and restore data, you must select a user account with the appropriate rights.



- For the File System iDataAgent, GroupWise iDataAgent and File Archiver for NetWare Agent, it is recommended that the user account have supervisor rights to the server.
- For the NDS iDataAgent, you must select a NetWare user account with supervisor rights to the root of the entire NDS tree.
- Changing a network account requires about five minutes to be synchronized.

Click **Next** to continue.

See the NetWare Server /DataAgents section in **User Accounts and Passwords** for more information.



You will be returned to Step to Destination Path for each server you have selected to configure for this custom installation. Once all of the servers have been configured, the install will continue.

## VERIFY SUMMARY OF INSTALL OPTIONS

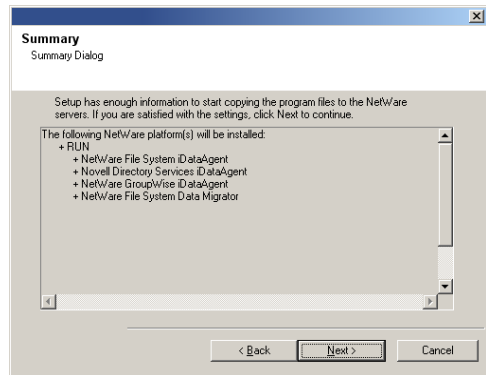
16. Verify the summary of selected options.

### NOTES

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

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

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



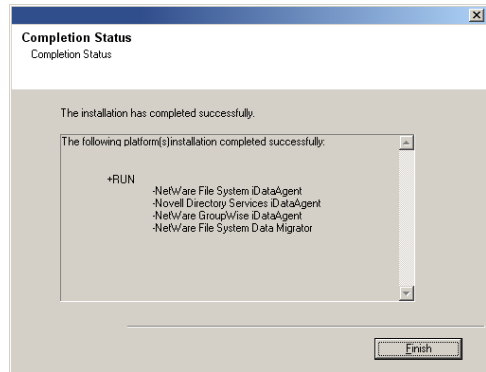
## SETUP COMPLETE

17. 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.

Click **Finish** to continue.



18. Click **OK** to exit the install program.

The installation is now complete.

### 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.



## POST-INSTALL CONSIDERATIONS

---

## GENERAL

- Install post-release updates or Service Packs that may have been released after the release of the software. When you are installing a Service Pack, ensure that it is the same version as the one installed in the CommServe Server. Alternatively, you can enable Automatic Updates for quick and easy installation of updates in the CommCell component.
- After installing the Agent, you may want to configure the Agent before running a data protection operation. The following list includes some of the most common features that can be configured:
  - Configure your subclients - see Subclients for more information.
  - Schedule your data protection operations - see Scheduling for more information.
  - Configure Alerts - See Alerts and Monitoring for more information.
  - Schedule Reports - See Reports for more information.

The software provides many more features that you will find useful. See the Index for a complete list of supported features.

---

## AGENT SPECIFIC

- The following configuration tasks are required before performing an Archive Operation using this Archiver Agent:
  - Create a Subclient - see Subclients - File Archiver for NetWare for more information.
  - Archiving Rules are initially disabled by default. You must clear the **Disable All Rules** option in the Subclient Properties (Archiving Rules) or (Rules) tab and configure the archiving rules before conducting rules-based Archive Operations.

---

## DISASTER RECOVERY CONSIDERATIONS

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

# Migration Archiving - File Archiver for NetWare Agent

Topics | How To | Related Topics

---

This feature/product/platform is deprecated in this release. See [Deprecated Features, Products, and Platforms](#) for more information.

Overview

How to Setup and Run a Migration Archive Operation

Protecting Stubs in Backups

Migration Archiving Considerations

- Encryption
- Filters
- Quotas
- Limitations
- General
- Stubs (Recovery, Icons, Recall Failures, Etc.)

Advanced Archive Options

---

## OVERVIEW

Migration Archiving of data allows preservation, transparent retrieval, and discovery of information held within a NetWare file system. Migration archiving reduces the size of data on the primary storage and decreases the duration of backup operations by the corresponding *iDataAgent*. Migrating data from file systems to secondary, tiered-storage maximizes storage utilization across the enterprise.

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

Migration archiving operations use:

- **Archiving Rules**

These rules specify criteria for the types of data to archive. These rules are configured on a per subclient basis. Rules are grouped by:

- **File Rules** - These rules relate to the low and high watermarks for free space on volumes as a basis for determining whether to scan a volume for archiving and to know when to stop archiving. For example, to scan a volume and start the archiving operation when the volume is low on free space and to stop the archiving after space has been freed up on the volume due to archiving. The rules also allow files to be archived based on a file's age and/or size.
  - **Stub Rules** - The stub rules allow you to determine when stubs are pruned and to disable stub creation altogether.
- 

## 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 still apply. See [Configure Archiving Rules - File Archiver Agents](#) 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, recover files with a non-browse recovery operation from a third party application, such as Windows Explorer (see [Recover a File from the NetWare System Console](#)).
    - If stubs were not created, then you can perform a browse recovery with CommCell Console (see [Recover a File from the CommCell Console](#)).
-

## PROTECTING STUBS IN BACKUPS

Stubs serve as placeholders for the data that is moved to secondary storage. Protecting stubs is useful to maintain the ability of non-browse recovery operations. For example, if there is a disk failure, the data can be restored along with the stubs. This reduces the size of the data in the volume as stubs consume less space.

These stubs are normally included in full backup operations by their NetWare file system *iDataAgent*.

---

### FILE ACCESS TIMES WHEN BOTH FILE ARCHIVER AND FILE SYSTEM IDATAAGENTS ARE INSTALLED

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

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

---

### INCLUDING STUBS IN INCREMENTAL BACKUPS

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

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

- Enable the **Check Archive Bit During Backups** option on the backup set of the associated File System *iDataAgent* prior to running the incremental backup. See Set the Archive Bit Attribute for step-by-step instructions.
- Enable the **Use Change Journal** option on the backup set of the associated File System *iDataAgent* prior to running the incremental backup. See Using Change Journal, Classic File Scan, or Data Classification Scan for Backups.

---

## MIGRATION ARCHIVING CONSIDERATIONS

Before performing any migration archiving procedures, review the following information:

---

### ENCRYPTION

- Before you can run a stub recovery operation of encrypted data (i.e., using pass-phrase security), you must export the pass-phrase to the local computer. Refer to Export an Encryption Pass-Phrase for the procedure to export the pass-phrase. If you have changed the encryption settings for your client since the data was archived, refer to Change Encryption Settings to understand potential impacts to recovery behavior.

---

### FILTERS

- Filters can be used with the **Items That Failed** list on the data protection **Job History Report** to eliminate backup or archive failures. Filters may be used to exclude items which consistently fail and 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.

- Application files/folders including software installation, magnetic mount path folders, databases, and mount path folders on which backup data resides should not be archived and must be manually filtered out.

---

### QUOTAS

- Do not set a quota for an object (such as a volume, directory, or user) that is lower than the amount already used. Doing so may cause improper results for data protection or recovery operations.

---

### LIMITATIONS

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

---

### GENERAL

- The software will report the same value for the size of the file(s) archived and the size of the disk. Thus, to determine the actual amount of space freed by the archive operation, you must compare the amount of free space available on the appropriate volume before and after the archive operation.

- Ensure that the migration archiving attribute is set on the NSS volume in order for files to be archived.

---

### STUBS (RECOVERY, ICONS, RECALL FAILURES, ETC.)

- If the stub cache is enabled, and if a stub file is recalled and the ACLs on the file are then modified, the changes to the ACLs are not picked up during the next migration archiving operation unless the file itself is modified. This is true because when a stub file is recalled under this scenario, a copy is put in the stub cache, and the file is copied back from the stub cache during the next migration archiving operation. The agent looks at the modified file time to determine if the file data has changed, and ACLs are not tracked by the modified file time when the stub cache is being used. As a workaround, modify the data in the file itself to pick up the changes made to its ACLs.

[Back to Top](#)

---

## Migration Archiving - File Archiver for NetWare Agent - How To

[Topics](#) | [How To](#) | [Related Topics](#)

---

### Migration Archive Options

[Enable\( Disable\) Archiving Rules](#)

[Configure Archiving Rules - File Archiver Agents](#)

[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 File Archiver for NetWare Agent.
- [User Account and Password - File Archiver for NetWare](#)

### 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 - FILE ARCHIVER AGENTS

### 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 File Archiver for NetWare Agent.
- User Account and Password - File Archiver for NetWare

#### Before You Begin

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

*Required Capability:* Capabilities and Permitted Actions

▶ To configure archiving rules for the File 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 File Rule tab (if not already selected).
    - a. Enable the Archiving Rules.
    - b. Configure the Archiving Rules.
  4. Click the Stub Rule tab and configure the Archiving Rules.
  5. Click **OK** to save your changes.
- 

## SCHEDULE A MIGRATION ARCHIVING OPERATION

#### Before you Begin

- See Overview for an introduction to the archiving rules and Migration Archiving Considerations for a list of considerations before you begin archiving with the File Archiver for NetWare Agent.
- After selecting your archiving options, you will be prompted to create a schedule for the migration archiving operation job. For more information, see Scheduling.

*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

- See Overview for an introduction to the archiving rules and Migration Archiving Considerations for a list of considerations before you begin archiving with the File Archiver for NetWare Agent.
- The migration archiving process allows you to archive data immediately without having to wait for the scheduled archiving time.

#### Before you Begin

*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

### Before you Begin

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

- 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

- See Overview for an introduction to the archiving rules and Migration Archiving Considerations for a list of considerations before you begin archiving with the File Archiver for NetWare Agent.
- Use the following procedure to start a migration archiving operation on new media. For more information, see Start New Media.

*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

### Before you Begin

- See Overview for an introduction to the archiving rules and Migration Archiving Considerations for a list of considerations before you begin archiving with the File Archiver for NetWare Agent.
- Use the following procedure to start a migration archiving operation that creates a new Index. For more information, see Create New Index.
- When you create a new index using this procedure, keep in mind that it will override the **Create new index every *n* archive operations** or **Set index cycle to every *n* archive jobs** setting in the Subclient Properties (Rules) tab, and the new index interval counter will start again at zero.

*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

### Before you Begin

- See Overview for an introduction to the archiving rules and Migration Archiving Considerations for a list of considerations before you begin archiving with the File Archiver for NetWare Agent.
- Use the following procedure to start a migration archiving operation that marks media full on completion. For more information, see Mark Media Full After Successful Operation.

*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

### Before you Begin

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

### Before you Begin

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

[Topics](#) | [How To](#) | [Troubleshoot](#) | [Related Topics](#)

---

This feature/product/platform is deprecated in this release. See [Deprecated Features, Products, and Platforms](#) for more information.

[Overview](#)

[How to Set Up and Run a Recovery Option](#)

[Recover a File from a NetWare System Console](#)

[Recover a File from Windows Explorer](#)

[Recovering Multiple Files from Stubs](#)

[Recall Throttling](#)

[Recovery Destinations](#)

- [In-Place Recovery](#)
- [Out-of-Place Recovery](#)
- [Recover to Network Drive/NFS-Mounted File System](#)

[Recovery Considerations for NetWare Agent](#)

---

## OVERVIEW

The File Archiver Agents support the following types of recoveries:

- Recovery of archived files per file paths provided using the CommCell Console.
- Browse and Recovery of archived files using the CommCell Console.
- Recall of archived files from stubs, using third-party applications (e.g., Windows Explorer, Unix Terminal or Console window, or NetWare System Console).

Recoveries can be performed in-place or out-of-place, and in certain scenarios cross-application recoveries and recoveries to a network drive or NFS-mounted file systems are also supported. (See, [Recovery Destinations](#) for comprehensive information.)

Recoveries using file paths for the File Archiver Agents can be performed from the archive set level in the CommCell Browser. Depending on the agent, browse and recovery operations for these agents can be performed from the client, agent, and subclient levels in the CommCell Browser.

When there is a problem with the file system, and/or operating system of the client computer full system restores may be required. The File Archiver Agents rely upon the corresponding File System iDataAgent to perform a full system restore of client data. See [Disaster Recovery](#) for more information.

[Back to Top](#)

---

## HOW TO SET UP AND RUN A RECOVERY OPTION

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 - File Archiver Agents](#) for step-by-step instructions.
2. Run an archive operation. See [Start a Migration Archiving Operation](#) for step-by-step instructions.
3. Optionally, if using stubs in your environment, decide if you want to throttle stub recovery requests. See [Recall Throttling](#) for more information.
4. Determine your Recovery Destinations.
5. Recover one or more files with a Browse and Recovery or recall operation.
  - If stubs were created, end-users or applications can recover files with a recall operation by simply opening the stub file, thereby causing it to be restored. (see [Recover a File from NetWare System Console](#)).
  - If stubs were not created, then you can perform a browse recovery with CommCell Console (see [Recover a File from the CommCell Console](#)).

[Back to Top](#)

## RECOVER A FILE FROM A NETWARE SYSTEM CONSOLE

The File Archiver for NetWare Agent provides several methods for recovering an archived file. Users can provide a path to the archived files to be recovered from the CommCell Console, perform a browse recovery for archived files from the CommCell Console or, if the subclient is configured to create stubs, perform a recall operation from a NetWare System Console. A recall is any action that causes an open and read to be executed for the archived file, which automatically initiates a recovery operation. One such example includes entering the `RECALL` command from the NetWare System Console.

For step-by-step instructions, see Recover a File from the NetWare System Console.

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 a File from the CommCell Console.

[Back to Top](#)

## RECOVER A FILE FROM WINDOWS EXPLORER

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 recall operation from a Windows workstation. A recall is any action that causes an open and read to be executed for the archived file, which automatically initiates a recovery operation. For example, clicking on the stub file from Windows Explorer.

- 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 a File from the CommCell Console.
- When a mount point contains stubbed files and it is moved, a reboot is required in order to recall the stubs.

For step-by-step instructions, see Recover a File from Windows Explorer.

[Back to Top](#)

## RECOVERING MULTIPLE FILES FROM STUBS

More than one archived file can be recovered at a time from stubs via a third-party application (e.g., Windows Explorer, Unix Terminal or Console window).







Multiple stub recoveries from disk media or tape are submitted to the Job Controller as one job. For such stub recoveries, only one job (i.e., called a *Persistent Recovery* job) will display in the Job Controller. However, the Event Viewer and Job History log will treat the jobs as separate jobs (using the same Job ID associated with the common open pipeline). Also, the job will wait for approximately 5 seconds in order to allow other stub recovery requests being submitted on the same client to be batched into the same job. It is worth noting that stub recoveries from disk media are faster than tape, because the pipeline remains open for up to 20 minutes of idle time, allowing quicker recovery and avoiding the time needed to find and load tapes.



For step-by-step instructions, see Recover Multiple Files from Windows Explorer.

[Back to Top](#)

## FILE ARCHIVER FOR WINDOWS STUB ICONS

When a file is archived with the create stub option enabled, offline attributes are set and the icon for the file will change to a special stub icon in Windows Explorer so that you can easily distinguish archived files. Some examples of commonly used stub icons are below:

	Adobe Acrobat Document
	JPG File
	Microsoft Excel Worksheet
	Microsoft Project Document
	Microsoft Word Document
	MP3 File

	Text File
	Text File (Windows 2008 or Windows Vista) (The displayed item is a product of Microsoft and beyond the control of this agent.)
no image	Due to limitations inherent in certain file types, including but not limited to *.html and *.tff files, no icons will be displayed in Windows Explorer for those files after archiving. This is normal for some files, and the stubs can still be recovered by clicking on the filename from Windows Explorer.

After a stub has been recovered, the icon will change back to the normal icon for the respective file type. Keep in mind that the File Archiver for Unix Agent does not support stub icons.

[Back to Top](#)

## RECALL THROTTLING

The number of stub recovery requests that can be run on an agent can be limited within a specified timeframe. Limits can be established that not only optimize performance but can also prevent the inadvertent recovery of a large number of files. Setting the recall throttling parameters involves configuring the maximum number of recalls, interval, and cool-down period for the agent. These parameters are entered on the Agent Properties dialog box.

See Set Stub Recovery Parameters for step-by-step instructions.

Examples are provided below to illustrate how this feature functions.

### SCENARIO

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

- Maximum Stub Recovery (i.e., limit) is set to 10
- Time Between Recall to Count as Successive in Seconds (i.e., interval) is set to 30 seconds
- Time to Wait after Maximum Successive Recalls Limit is Reached in Seconds (i.e., cool-down) is set to 60 seconds

#### EXAMPLE 1 - MAXIMUM LIMIT IS NOT EXCEEDED (WITH NO ADDITIONAL RECALL REQUESTS)

**Action:** A user submits 4 stub recovery requests at the same time on a given client, and no other stub recovery requests are submitted on that client during the 30 second interval that follows.

**Result:** As each stub recovery request is received, it will begin processing immediately and the 30 second interval countdown will begin where the system will wait to see if any more stub recovery requests are submitted. There is no cool-down period since the limit was not reached, and all 4 files will be recovered.

#### EXAMPLE 2 - MAXIMUM LIMIT IS EXCEEDED (WITH NO ADDITIONAL RECALL REQUESTS)

**Action:** A user submits 20 stub recovery requests at the same time on a given client, and no other stub recovery requests are submitted on that client during the 30 second interval that follows.

**Result:** The first 9 stub recoveries will begin immediately, the 30 second waiting interval does not apply here since the limit has been reached, and the 60 second cool-down period begins where no other stub recovery requests will be accepted. Note that 11 stub recovery requests (out of 20) that were over the limit will not be processed, and an event will be issued in the CommCell Console's Event Viewer and the Windows Event Viewer indicating that the limit has been reached. The first 9 files will be recovered, and depending on the agent the user will see one of the following results for the 11 stub recovery requests that were over the limit:

*File Achiver for NetWare:* Assuming they were text files, 11 Notepad sessions appear on the desktop with each containing a message indicating that this is a stub file.

#### EXAMPLE 3 - MAXIMUM LIMIT IS NOT EXCEEDED (WITH ADDITIONAL RECALL REQUESTS RECEIVED WITHIN THE INTERVAL)

**Action:** A user submits 4 stub recovery requests at the same time on a given client, and 4 other stub recovery requests are submitted on that client by another user during the 30 second interval that follows.

**Result:** As each stub recovery request is received from the user, it will begin processing immediately and the 30 second interval countdown will begin where the system will wait to see if any more stub recovery requests are submitted. After 20 seconds have elapsed, the 4 additional stub recovery requests are received so the 30 second interval countdown will begin again (i.e., the count is initialized to zero) to allow one more request to be submitted. Since the limit has not been reached, the cool-down period does not apply, and all 8 files will be recovered on a first-in first-out basis.

#### EXAMPLE 4 - MAXIMUM LIMIT IS NOT EXCEEDED (WITH ADDITIONAL RECALL REQUESTS RECEIVED OUTSIDE THE INTERVAL)

**Action:** A user submits 4 stub recovery requests at the same time on a given client, and 8 additional stub recovery requests are submitted on that client by another user 35 seconds later.

**Result:** As each stub recovery request is received from the user, it will begin processing immediately and the 30 second interval countdown will begin where the system will wait to see if any more stub recovery requests are submitted. After 35 seconds have elapsed, 8 additional stub recovery requests are received and the 30 second interval countdown will begin again (i.e., the count is initialized to zero) to allow one more request to be submitted. Since the limit was never reached during the first or second interval, the cool-down period does not apply, and all 12 files will be recovered on a first-in first-out basis.

[Back to Top](#)

---

## RECOVERY DESTINATIONS

By default, data is recovered 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 sections enumerate the types of recovery destinations that are supported. 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 recall 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.

When performing an In-Place Recovery for Recovery-by-Job the user has to provide the login credentials for FPolicy and Network File Share Instance.

---

### OUT-OF-PLACE RECOVERY

- Same path/destination
- Different path/destination

Consider the following when performing out-of-place recoveries:

- Out-of-place recoveries can only be accomplished via a Browse and Recovery operation from the CommCell Console.
- When performing an out-of-place recovery, the only requirement for the destination computer is that it must have a compatible File System iDataAgent installed (i.e., does not need to have a File Archiver Agent installed).

---

### CROSS-PLATFORM RECOVERIES

- Same Operating System - Different Version

When performing a cross-platform recovery of archived data from a newer version of an operating system to an older version, keep in mind that some file attributes/properties native to the newer version may not be recovered to the older version.

Consider the following when performing cross-platform recoveries:

- Cross-platform recoveries can only be accomplished via a Browse and Recovery operation from the CommCell Console.

---

### RECOVER TO NETWORK DRIVE/NFS-MOUNTED FILE SYSTEM

Besides recovering data to a client computer's local drive, you can also recover data to a UNC path (Windows) or NFS-mounted file system (Unix) depending on your agent. (See [Restore to Network Drive/NFS-Mounted File System](#) for comprehensive information.)

Consider the following when recovering archived data:

- The File Archiver for Windows/NetWare Agents support recoveries to a mapped network drive (e.g., UNC path), but not to an NFS-mounted file system.

---

### MOVED STUBS

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

[Back to Top](#)

---

## RECOVERY CONSIDERATIONS FOR NETWARE AGENT

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

---

### COMMON

- Do not set a quota for an object (such as a volume, directory, or user) that is lower than the amount already used. Doing so may cause improper results for data protection or recovery operations.
- If the CommServe and the Agent are upgraded as a result of existing license expiry or new license application, Stub Recalls will not occur. You need to

perform Browse and recover from the CommCell Console to recover the archived files.

- To avoid losing changes to alternate streams after stubbing use `GXHSM_IGNORE_ALT_STREAM_RECALLS` key.

---

## FILE ARCHIVER FOR NETWARE AGENT

- Files that have been recalled but have not been changed are not re-archived in their entirety during the next archive operation, provided the files continue to meet the migration rules. Instead, these files will be re-stubbed during the next archive operation. As a result, time is saved during the next archive operation and archive media space is saved by not containing duplicate copies of identical files.
- By default no failure message is displayed when a recall job waits for the media to be imported. Use `DMReadMaxMountRetryVal` key allows for setting a finite number of mount retries during restore.

[Back to Top](#)

---

# Recover Data - File Archiver for NetWare Agent - How To

[Topics](#) | [How To](#) | [Troubleshoot](#) | [Related Topics](#)

---

## Recovering Data

[Recover a File from the CommCell Console](#)

[Recover a File from Windows Explorer](#)

[Recover Multiple Files from Windows Explorer](#)

[Recover a File from the NetWare System Console](#)

[Set Stub Recovery Parameters](#)

## Recovery Destinations

[Recover Out-of-Place or Cross-Platform](#)

[Recover to a Network Drive/NFS-Mounted File System](#)

---

## RECOVER A FILE 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 a file from the CommCell Console:

1. From the CommCell Browser, right-click the agent, backup set, or subclient whose data you want to browse, click **All Tasks** (if displayed), and then click the desired **Browse** option.
2. From the Browse Options dialog box, select the browse options that you want to use.
3. If specifying a browse time, click **Advanced** for the Advanced Browse Options.
4. From the Browse window, select the file(s) you want to recover, then click **Recover All Selected**.
  - Click **New Browse** to initiate a fresh browse window. Use new browse option settings if desired.
  - To search for a particular file, refer to [Find a File/Directory/Object](#) for instructions.
5. From the **Restore/Recover Options (General)** and Job Initiation tabs, select the desired recovery options.
6. When restoring encrypted data, refer to [Data Encryption](#).
7. Click **Advanced** to select advanced recovery options for the job.
8. Click **OK** on the Recover Options dialog box.
9. A recovery job is started for the selected data and indicates its status in the Job Controller window.
10. When the recovery has completed, a confirmation message will be displayed in the Job Controller window.

---

## RECOVER A FILE FROM WINDOWS EXPLORER

**Before You Begin**

- Review Recover a File from Windows Explorer.
- 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.
- If you want to enable/disable the pop-up message to confirm when then stub recovery operation has completed and to show the location of the file, see Recovery Considerations for these Agents for more information.

*Required Capability:* See Capabilities and Permitted Actions

▶ To recover a file from Windows Explorer:

1. Log on to the client computer from which the file was archived, or a computer that has a mapped network drive to the volume where the stub resides.
2. Locate the file stub in Windows Explorer, then double-click the stub to begin the recovery operation.

If the pop-up confirmation message feature has been enabled, a window will display the location of the file that will be recovered. Once the recovery operation has completed, the pop-up will close automatically. For remote recoveries using File Archiver for Windows, another pop-up will appear on the remote workstation indicating that the recovery operation has completed. Click **OK** to close the window.

**RECOVER MULTIPLE FILES FROM WINDOWS EXPLORER****Before You Begin**

- Review Recovering Multiple Files from Stubs.
- Review the general recovery requirements from What You Need to Know Before Performing a Recovery and any agent-specific recovery requirements from prior to performing any recovery.
- If you want to enable/disable the pop-up message to confirm when then stub recovery operation has completed and to show the location of the file, see Recovery Considerations for these Agents for more information.

*Required Capability:* See Capabilities and Permitted Actions

▶ To recover multiple files from Windows Explorer:

1. Log on to the client computer from which the files were archived, or a computer that has a mapped network drive to the volume where the stubs reside.
2. Locate the file stubs in Windows Explorer, then use **Ctrl** + click to select the stubs to be recovered.
3. Press **Enter** (or select **Open** from the File pull-down menu or right-click menu) to begin the recovery operation.

If the pop-up confirmation message feature has been enabled, a window will display the location of the latest file that was submitted for recovery. Once the recovery operation has completed, the pop-up will close automatically. For remote recoveries using File Archiver for Windows, the number of pop-ups on the remote workstation will be equal to the number of stub recoveries submitted and each will indicate that the recovery operation has completed. Click **OK** to close each window.

**RECOVER A FILE FROM THE NETWARE SYSTEM CONSOLE****Before You Begin**

- Review Recover a File from a NetWare System Console.
- 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 an archived file from the NetWare system console:

1. Access the system console on the NetWare Server where the archived files reside.
2. From the system console prompt, execute any command that performs an open and read on the archive file that you want to recover. For example, you can use the **EDIT** command in a couple of ways to do this:
  - **EDIT** <path><filename> then press **Enter**.
  - **EDIT** then press **Enter**. From the system editor, browse to the archived file you want to recover then click on the file to open it.
3. The recovery job is submitted to the Job Controller, and you can track the status of the job from the Job Controller window in the CommCell Console.

**SET STUB RECOVERY PARAMETERS****Before You Begin**

- Review information about Recall Throttling before beginning this procedure.

*Required Capability:* See Capabilities and Permitted Actions

▶ To set stub recovery parameters:

1. From the CommCell Browser, right-click the appropriate agent icon and then click **Properties**.
2. From the General tab of the Agent Properties dialog box, click the **Stub Recovery Parameters** option.
3. Select the appropriate value for the **Maximum Stub Recovery** field.
4. Select the appropriate value for the **Time between recall to count as successive in seconds** field.

The interval value for FPolicy, NAS data, and Celerra should be set to 200 for complete Recall Throttling effect.

5. Select the appropriate value for the **Time to wait after maximum successive recalls limit is reached in seconds** field.
6. Click **OK**, then either wait 5 minutes for the change to take effect or restart the DataArchiver service for it to take effect immediately.

## RESTORE OUT-OF-PLACE, CROSS-PLATFORM OR CROSS-APPLICATION

### Before You Begin

- Review the general and agent-specific restore requirements accessed from Restore Backup Data prior to performing any restore operation.

*Required Capability:* See Capabilities and Permitted Actions

▶ To browse and restore data:

1. Begin any restore procedure. See Basic Restore or Browse and Restore\_for step-by-step instructions.
2. From the agent's **Restore Options** dialog box, select the restore destination:
  - **Destination Computer** - By default, data is restored to the same computer from which it was backed up. To change the destination computer, select one from the list. The list includes established clients within the CommCell, with Operating Systems that support the out-of-place, cross-platform, or cross-application restore operation from this client.
  - **Restore to Same Paths** - Specifies whether the restore operation must restore data to the **Destination Computer** using the same path from which it was backed up. Clear this option if you want to restore to a different path and activate the **Destination folder** box.
  - **Destination Folder** - Use this space to enter (or browse to) the path on the destination computer to which the data must be restored. If the specified path does not exist, it will be created during the restore process.

On Windows computers, the UNC path of a shared drive can be specified. (e.g., \\servername\sharename\directory). Deselect **Restore to Same Paths** and then type the UNC path of the shared drive in the **Destination Folder** field.

3. After completing your selections, continue with the restore procedure.

## RECOVER OUT-OF-PLACE OR CROSS-PLATFORM

### Before You Begin

- Review the general and agent-specific recovery requirements accessed from Recover Archived Data prior to performing any recovery operation.

*Required Capability:* See Capabilities and Permitted Actions

▶ To browse and recover data:

1. Begin a browse and recovery procedure from the CommCell Console. See Recover a File from the CommCell Console for step-by-step instructions.
2. From the agent's **Recover Options** dialog box, select the recovery destination:
  - **Destination Computer** - By default, data is recovered to the same computer from which it was archived. To change the destination computer, select one from the list. The list includes established clients within the CommCell, with Operating Systems that support the out-of-place or cross-platform recovery operation from this client.
  - **Recover to Same Paths** - Specifies whether the recovery operation must recover data to the **Destination Computer** using the same path from which it was archived. Clear this option if you want to recover to a different path and activate the **Destination folder** box.
  - **Destination Folder** - Use this space to enter (or browse to) the path on the destination computer to which the data must be recovered. If the specified path does not exist, it will be created during the recovery process.

On Windows computers, the UNC path of a shared drive can be specified. (e.g., \\servername\sharename\directory). Deselect **Recover to Same Paths** and then type the UNC path of the shared drive in the **Destination Folder** field.

3. After completing your selections, continue with the recovery procedure.



---

## RESTORE TO A NETWORK DRIVE/NFS-MOUNTED FILE SYSTEM

### Before You Begin:

- On Windows computers, shared network drives exist as Windows share directories (i.e., shares) on some other computer on the network. For data security reasons, these shares possess access privileges that determine who can access the share and the rights under which access is permitted. If your Windows account does not have privileges to write data to the share, you must be prepared to provide the login and password of a Windows account that does have these privileges.
- For Unix computers, ensure that the destination computer has root permissions for the NFS-mounted file system. If the destination computer does not have these permissions, restores will fail.
- Ensure that the network drive / mounted file system to which you intend to restore the data is accessible as a mapped network drive/ NFS-mounted file system from the destination computer.
- Review the general and agent-specific restore requirements accessed from Restore Backup Data prior to performing any restore operation.

*Required Capability:* See Capabilities and Permitted Actions

▶ To browse and restore data using wildcards:

1. Begin any restore procedure. See Basic Restore or Browse and Restore\_for step-by-step instructions.
2. From the **Restore Options** dialog box, ensure that the **Destination Computer** is the source computer from which the shared drive was backed up, not the computer that has the share. If the data did not originate from the shared drive, de-select **Restore to Same Paths** and then type the UNC path of the shared drive in the **Destination Folder** field (e.g., \\servername\sharename\directory).
3. To restore to a Windows computer, click **Advanced**.

If you do not have Change permissions for the share to which you intend to restore the data, then you must select **Impersonate NT User** in the **Advanced Restore Options** dialog box and provide the login and password of a Windows account that does have these permissions. (Otherwise, the data cannot be restored to the selected share. Ordinarily, if you can copy or create a file in the share, you should be able to restore data to that share without having to select this option.)

If the user account is established as a domain user account, you must enter a fully qualified user name (e.g., <domain\_name>\<user\_name>) and password.

4. Optionally select the additional restore options that you want to use from the **Advanced Restore Options** dialog box.
5. Click **OK**.
6. Optionally select the additional restore options that you want to use from the **Restore Options** dialog box.
7. Click **OK**.
8. After completing your selections, you can either start an immediate restore or schedule the restore.
  - If you want to schedule the job, click the Job Initiation tab from the Restore Options dialog box, click **Schedule**, and enter your selections in the Schedule Details (Schedule Details) dialog box. Clicking **OK** from this dialog box saves your schedule. See Scheduled Data Recovery Operations for an overview of this feature.
  - 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.

### NOTES

- The restored data assumes the access characteristics of the destination share.
- In the case of a File Level restore using the Image-Level iDataAgent, the restored data assumes the access characteristics of the destination share.

---

Back To Top

# Agents - File Archiver for NetWare

[Topics](#) | [How To](#) | [Related Topics](#)

---

This feature/product/platform is deprecated in this release. See [Deprecated Features, Products, and Platforms](#) for more information.

- [Configurable Properties](#)
  - [Activity Control](#)
  - [Assigning a Filter Storage Policy for Erase Data by Browsing](#)
  - [Setting the Upper Limit for Maximum Stub Recovery](#)
  - [User Accounts](#)
  - [User Security](#)
  - [Version](#)
- 

## 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 tabs that are available for that agent in the 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](#).

---

## SETTING THE UPPER LIMIT FOR MAXIMUM STUB RECOVERY

For the File Archiver Agents, you can enable recall throttling to limit the maximum number of stubs that can be recovered by an agent within a specified timeframe. See [Recall Throttling](#) for an overview.

---

## USER ACCOUNTS

Displays the user account used by the system to log in to or access the (the tree of the) server during various jobs (including backups, browses, restores, etc.). See [Network Server iDataAgents](#) 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.

---

# Agents - File Archiver for NetWare - How To

[Topics](#) | [How To](#) | [Related Topics](#)

---

Assign a Filter Storage Policy for Erase Data by Browsing

Run Erase Data by Browsing Job

Set Stub Recovery Parameters

Release License for Client, MediaAgent, Agent, or Enabler

Delete the Agent

View the Software Version

---

## 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**.
- 

## 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.
- 

## SET STUB RECOVERY PARAMETERS

### Before You Begin

- Review information about Recall Throttling before beginning this procedure.

*Required Capability:* See Capabilities and Permitted Actions

▶ To set stub recovery parameters:

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

2. From the General tab of the Agent Properties dialog box, click the **Stub Recovery Parameters** option.
3. Select the appropriate value for the **Maximum Stub Recovery** field.
4. Select the appropriate value for the **Time between recall to count as successive in seconds** field.

The interval value for FPolicy, NAS data, and Celerra should be set to 200 for complete Recall Throttling effect.

5. Select the appropriate value for the **Time to wait after maximum successive recalls limit is reached in seconds** field.
6. Click **OK**, then either wait 5 minutes for the change to take effect or restart the DataArchiver service for it to take effect immediately.

---

## 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.

---

# Archive Sets - File Archiver for NetWare Agent

Topics | How To | Related Topics

---

This feature/product/platform is deprecated in this release. See [Deprecated Features, Products, and Platforms](#) for more information.

Overview

Configurable Properties

- Backup Set/Archive Set Name
  - User Security
- 

## OVERVIEW

After installation, the system automatically creates a default archive set. See [Archive Sets](#) for information on the different types of archive sets.

---

## FILE ARCHIVER FOR NETWARE AGENT CONFIGURABLE PROPERTIES

Once installed, a user-defined subclient must be configured for each archive set in order to manage the data or volumes on the client computer. Each Archive Set has properties that can be configured 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.

---

### 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 - File Archiver for NetWare Agent - How To

Topics | How To | Related Topics

---

[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](#)

---

## 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 iDataAgent 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 *iDataAgent*, you can add/modify an application/database user account. See the DB2 *iDataAgents* 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.
-



# Subclients - File Archiver for NetWare

Topics | How To | Related Topics

This feature/product/platform is deprecated in this release. See [Deprecated Features, Products, and Platforms](#) for more information.

Overview

Subclient Content

Configurable Properties

Things to Consider when Creating and Configuring Migration Archiver Subclients

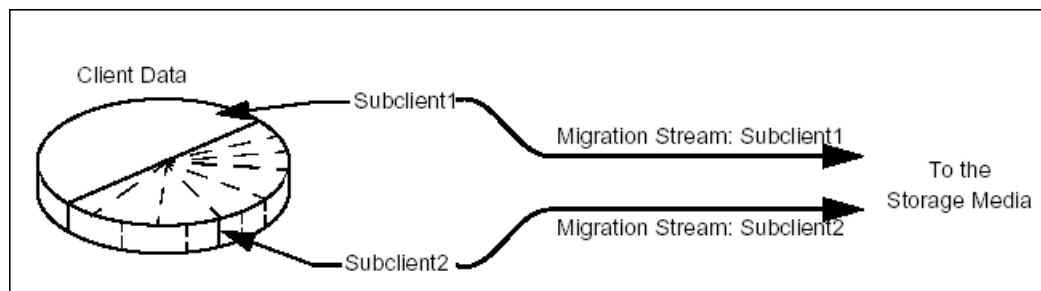
- Common
- File Archiver for NetWare Agent

## 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
File Archiver for NetWare	NetWare files	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

### FILE ARCHIVER FOR NETWARE AGENT

The File Archiver for NetWare agent is designed to archive unused or infrequently used NetWare File System data from a host computer to secondary storage and to recover this data. Subclient content for this agent includes the appropriate NetWare File System (UFS) data per the supported platform. Some related data types are not recommended for archiving, while other data types are automatically filtered out of archive operations by the system and cannot be archived. For more information on what data types are supported or not supported, see [Supported Data Types](#).

After you install this agent, a default subclient is not automatically created; you must create a user-defined subclient, and you must select the content for this subclient by configuring the **Subclient Properties (Content)** tab from the CommCell Console. Thereafter, you can create additional user-defined subclients to archive additional data if desired.

When you configure subclient content, you browse the directory tree structure on the client computer and select the directories and files that you want protected. The resulting content will display the selected items. For example:

```
volume name:\tests
```

volume name:\trials

volume name:\results

A useful way to distribute subclient content of a File Archiver for NetWare agent is by directory or groups of directories, as shown in this example:

- User-defined subclient: tests  
Content: volume name:\tests
- User-defined subclient: trials  
Content: volume name:\trials
- User-defined subclient: results  
Content: volume name:\results

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

## FILTERING

Subclient-level archive filters are available for this agent to exclude specified directories and files from being archived. For example, suppose the `Ops` directory contains a file called `Processing` that you do not want archived. You can add a subclient filter for the user-defined subclient `OpsInfo` to exclude the `Processing` file from being archived. Subclient-level archive filters are also available for this agent to provide exceptions to the data that you are excluding. For example, suppose that you want to exclude from your migration archive operation all the files in the `Ops` directory except the `Maintenance` file. You can add a subclient filter for the user-defined subclient `OpsInfo` to exclude the `Ops` directory from being archived, but you can add a corresponding subclient filter to allow the `Maintenance` file to be archived. For more information, see [Filters](#).

## WILDCARDS AND REGULAR EXPRESSIONS

Wildcards and regular expressions are supported by this agent in the following function:

- Subclient Filters Wildcards can be used in the `Exclude these files/folders/patterns` field when filtering data using subclient-level archive filters.

Wildcards are not supported in Exception filters.

For this agent, the exception filter is represented by the `Include these files/folders/patterns with every archive field`.

For a list of wildcards supported by this agent, see [Wildcards](#).

## 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 \(Rules\)](#).

---

## 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.

Only the Exchange Mailbox Archiver Agent supports the ability to edit data protection filters, whereas the Exchange Public Folder Archiver Agent does not.

---

## **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 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](#).

The Security tab is not available for File Archiver Agents at the subclient level.

---

## **THINGS TO CONSIDER WHEN CREATING AND CONFIGURING MIGRATION ARCHIVER SUBCLIENTS**

When creating and configuring subclients for Migration Archiver Agents, 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](#).

---

### **FILE ARCHIVER FOR NETWARE AGENT**

- Subclient content is defined at the folder/directory/volume level.
- Since default subclients are not supported, you will have to create a user-defined subclient after installing the agent in order to perform migration archiving operations. During subclient creation, you will specify which portion of the client's folders/directories/volumes will be scanned for archiving by the subclient.

- It is not recommended to specify Volumes that contain disk library mount paths for subclient content; otherwise, the entire disk library will be archived. The subclient filter does not currently allow disk library mount paths to be filtered out of subclient content.

[Back to Top](#)

---

## Subclients - File Archiver for NetWare - 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/vol10/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:
  - o Click the upper **Add** button.
  - o From the Browse window, expand the mailbox tree of the client computer.
  - o 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.)
  - o 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 iDataAgents, 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 iDataAgents, 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:
  - o 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.
  - o 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 iDataAgents and SharePoint Server iDataAgent, to specify a workspace/folder that you want to exclude from the backups, click the upper **Browse** button and expand the iDataAgent 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 iDataAgents, File Archiver for Windows/Unix Agents, and ProxyHost iDataAgent, to specify a file/folder/directory that you want to exclude from data protection operations, do one of the following:
  - o 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.
  - o 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 iDataAgents, to specify data that you want excluded from the backups, do one of the following:
  - o 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.
  - o 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 iDataAgents, to specify a file or folder that you want to exclude from discovery, do one of the following:
  - o 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.
  - o 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:
  - o Click the lower **Add** button.
  - o In the Input window, type the wildcard pattern of the folders that you want to exclude from backup/archive operations on the selected subclient.
  - o 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 iDataAgents and SharePoint Server iDataAgent, 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

*iDataAgent* 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 *iDataAgents*, File Archiver for Windows/Unix Agents, and ProxyHost *iDataAgent*, 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:
  - o 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.
  - o 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 *iDataAgents*, 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:
  - o 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**.
  - o 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 *iDataAgents* 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 *iDataAgent*, 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 *iDataAgent*, 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 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 *iDataAgents* 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 *iDataAgents*: 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 *iDataAgent*: 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 *iDataAgent*: 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 *iDataAgents*, NDS, and SharePoint Server *iDataAgents* 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 *iDataAgents*: 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 *iDataAgents*: Click **Browse**, select folders to include as content, then click **Add**.
    - For the Unix File System *iDataAgents*, to facilitate the management of resource fork data in Apple double-encoded Macintosh files, click **Enable Apple Double Support**.
    - For the Unix File System *iDataAgents*, 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 *iDataAgents*, 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 iDataAgents 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 iDataAgents, click the Subclient Properties (Content) tab and configure content for the subclient as described below for your agent:

- For the DB2 iDataAgent, specify whether you want to include the entire database or a subset of this data as content for the subclient. For the DB2 DPF iDataAgent, 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 iDataAgents: 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 iDataAgent, follow the procedure to Discover and Assign New Data Types.
- For the Sybase iDataAgent, follow the procedure to Manually Discover Databases.
- For the MySQL iDataAgent, follow the procedure to Configure MySQL Databases.

- For the Informix iDataAgent, 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 iDataAgent, 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 iDataAgents, click the Subclient Properties (Content) tab and configure content for the subclient as described below for your agent:

- Image Level on Unix iDataAgent: 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 iDataAgents: 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 iDataAgent: 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 *iDataAgent*:
  - `/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 *iDataAgents* 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 *iDataAgent*: 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 *iDataAgent*: 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 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 *iDataAgents* 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 *iDataAgents*: 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 *iDataAgent*: 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 *iDataAgent*: 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 *iDataAgents*, NDS, and SharePoint Server *iDataAgents* 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 *iDataAgents*: 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 *iDataAgents*: Click **Browse**, select folders to include as content, then click **Add**.
- For the Unix File System *iDataAgents*, to facilitate the management of resource fork data in Apple double-encoded Macintosh files, click **Enable Apple Double Support**.
- For the Unix File System *iDataAgents*, 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 *iDataAgents*, 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 *iDataAgents* 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 *iDataAgents*, click the Subclient Properties (Content) tab and configure content for the subclient as described below for your agent:

- For the DB2 *iDataAgent*, specify whether you want to include the entire database or a subset of this data as content for the subclient. For the DB2 DPF *iDataAgent*, 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 *iDataAgents*: 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 *iDataAgent*, follow the procedure to Discover and Assign New Data Types.
- For the Sybase *iDataAgent*, follow the procedure to Manually Discover Databases.
- For the MySQL *iDataAgent*, follow the procedure to Configure MySQL Databases.
- For the Informix *iDataAgent*, 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 *iDataAgent*, 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 *iDataAgents*, click the Subclient Properties (Content) tab and configure content for the subclient as described below for your agent:
  - Image Level on Unix *iDataAgent*: 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 *iDataAgents*: 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 *iDataAgent*: 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 *iDataAgent*:
  - `/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 *iDataAgents* 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 *iDataAgent*: 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 *iDataAgent*: 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 *iDataAgents*: 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 *iDataAgents*: 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 *iDataAgent* also requires that you set permissions for the batch/shell script file on the backup host.

- SQL Server Database *iDataAgents*: When running on Windows Server 2003 and VSS is enabled, the **New Subclient** command is not available.
- PostgreSQL *iDataAgents*: 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 *iDataAgent*, 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 *iDataAgents* 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.
  - o For the DB2 and DB2 DPF *iDataAgents*, you can also change the number of data backup streams. For the DB2 DPF *iDataAgent*, the default stream threshold should be equal to the total number of database partitions for the subclient.
  - o For SQL Server *iDataAgents*, 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.
  - o 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 *iDataAgents*, 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 *iDataAgents*, 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.
  - o 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**.
  - o 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**.
  - o 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**.
  - o 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 iDataAgent, 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**.

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

- From the CommCell Browser, right-click the subclient whose Global Filter you want to disable, and then click **Properties** from the shortcut menu.
- Click the Filters tab of the Subclient Properties dialog box.
- 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.
- 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:

- 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.
- Click the Filters tab of the Subclient Properties dialog box.
- 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 *iDataAgents*, 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 *iDataAgents*, 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 *iDataAgents* and SharePoint Server *iDataAgent*, to specify a workspace/folder that you want to exclude from the backups, click the upper **Browse** button and expand the *iDataAgent* 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 *iDataAgents*, File Archiver for Windows/Unix Agents, and ProxyHost *iDataAgent*, 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 *iDataAgents*, 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 *iDataAgents*, 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 *iDataAgents* and SharePoint Server *iDataAgent*, 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 *iDataAgent* 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 *iDataAgents*, File Archiver for Windows/Unix Agents, and ProxyHost *iDataAgent*, 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 *iDataAgents*, 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 were found for the backup, 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 window, 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 iDataAgents. 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 were found for the backup, 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](#)